THE LIFECYCLE MODEL FOR CLOUD GOVERNANCE

Yu He

Assigned by:

logica
be brilliant together

WORKING TOMORROW
TO TRY IS TO LEARN

UNIVERSITY OF TWENTE. 50

Master Thesis

The Lifecycle Process Model for Cloud Governance

Author

Yu He

Program	Msc. Business Information technology
Student Number	S1024221
E-mail	y.he-2@student.utwente.nl

Graduation Committee

Maria Eugenia Iacob

Department	University of Twente, Information System & Change Management
Email	m.e.iacob@utwente.nl

Marten van Sinderen

Department	University of Twente, Computer Science
Email	m.j.vansinderen@utwente.nl

René Kleizen

Department	Logica , Working Tomorrow
Email	rene.kleizen@logica.com

Management Summary

The concept of cloud computing has gained much attention in recent years. Cloud computing enables organizations to scale and change their services easily. However, the new business model drives client organizations to reevaluate their current processes and structure for the control. Cloud governance is a new concept established to cope with the control issues regarding the cloud services and to ensure that organizations can realize their business value in a more flexible way through cloud. Since cloud adoption is in the early stage, our model proposes a lifecycle approach to enable organizations to implement their governance incrementally.

This thesis starts from comparison of literatures on SOA governance and Cloud governance, from which five governance areas are derived. The model follows a lifecycle approach and each phrase focuses on a different part of cloud governance. The whole process model is triggered by the process of defining goal for cloud computing. The arrows in our high-level process indicate some causality relationship between the phrases but they do not imply the chronological order. Each process is accompanied with method suggestions and deliverables to make it executable. The highlighted processes indicate that there are some differences between SOA and cloud in those processes. Besides some variations with respect to types of cloud are discussed, however, due to the time limitation the discussions are kept in a higher level.

To increase the practical relevance of this model, a series of interviews covering IaaS, PaaS, and SaaS service have been conducted to show the current state of cloud governance in practice. It turns out that most of the organizations concentrate on contract management. Organizational structure and processes are not yet transformed in most of organizations. From the result of the interviews, we find out that our model basically includes the important parts on cloud governance. In accordance with the interview results, four new processes have been added into our model and one process method has been revised.

From our research, some suggestions and findings to ensure successful cloud implementation are made:

- Pay more attention to public cloud
- Ensure TCO is in place before cloud is introduced and start pilots projects on non-critical application
- Cloud coordinator will facilitate cloud adoption
- IT roles should shift to contract management and information management

- Testing security on cloud will be difficult
- Delegate incident management and low level configuration management to suppliers , take care of change management
- Establish policy management process internally and externally
- Monitoring SLA can depend on third party organization to avoid upfront investment
- Introduce a self-service portal and registry/repository to support governance
- Whether business continuity plan should delegate to suppliers depends on TCO
- Evaluate service to compensate lost
- Arrange exit plan to avoid vendor lock-in
- Unify the control mechanisms in general

Further Researches

We see several improvements which can be made to our lifecycle model in the future:

- Further tailor the processes to each type of cloud service, especially for SaaS
- Link the roles and processes to clarify the responsibility
- Develop a maturity model to guide organizations to implement the governance gradually
- Take the auditor perspective to investigate contents for auditing cloud suppliers

Preface

Last year in November I received the internship offer from Riccardo and I was told that my assignment had something to do with cloud governance. At the moment I felt really excited and looked forwards to the new life and research in industry on the most fashionable IT concept – "cloud computing". Frankly, I had no idea what cloud computing is but the basic IT service that can be acquired like electricity at that time. Since then I started my long journey to explore the essence of cloud computing and its governance mechanisms.

Taking the time to look back at all the results and experience I have received, I believe that my objective has been reached. I have to say that the six-month internship period is the most challenging period of my study in Netherlands. During the time I have to get myself involved into a Dutch working environment, specify the assignment, arrange interviews, and manage my a good quality deliverable within a tight timeframe. Now seeing that my thesis has been finished on time, the experience and skills I have gained, friends I have made and a lot of activities I have joined in, I can proudly announce that I have succeeded my challenging phrase of my life .The research would have never approached its closure without the support and feedback from people around me.

For University of Twente, my supervisors help me out tremendously. First, I would like to thank Maria Iacob, who suggests me to look into the SOA governance approaches and to investigate them for cloud computing. Her advices and own experience as an international student have encouraged me and helped me a lot and kept me continue with my research when I was in a dilemma. Marten van Sinderen, a gentleman I have never met before, walks me through the time when I have questions on my research. I am really grateful for their instructions and assistance during the whole period.

For Logica, I am grateful for the helps I have received from all the people at Logica throughout my internship. Specifically I want to thank Rene Kleizen, who supervised my daily work and progress in Logica. He was always ready to help me go through all the difficulties, introducing me to various people within and outside Logica for my research, assisting me to get blended into the whole working environment and WT team. I would like to thank Riccardo Becker, who offered the assignment and respected me for my final choice on the research direction. I have to say sorry to him because my final research direction deviated from what he wanted at the very beginning. I am grateful for his willingness to spend time to discuss on my new direction. I am also very grateful for the assistance from Peter Vruggink and Freek Uijtdewilligen.

Of course I own a lot of thanks to all the people who was willing to accept my interviews. You are so kind and supported to spend your own time for an international student. Some of you I just know from the Internet and I am really surprised that you were willing to offer help to such a green student in a kindly manner. Thank you all, Joey Joosten, Robbert Schravendijk, Ruud Ramakers, Roald Kruit, Buve Franc, Wil Janssen, and Maurice van der Woude.

Finally, I would like to thank my family and all my friends, who gave a lot of mental supports to me during the whole six months. Duc, Priscilla, Ravi, Eyla, Mario, and Wei, thank you for checking my work and your comments. Yanting, Haihan and Wei, thanks for the delicious food. You are my family in the Netherlands.

Arnhem, June 17th 2011

Yu He

Content

List of Figures

List of Tables

1 Introduction

This chapter presents the research setting, motivation, research objective, research questions and research approach.

1.1 Research Setting

This research takes at Logica, Arnhem. Logica is a major international player in the field of IT and business services with 39,000 employees in 36 countries. It provides solutions and services in the field of consultancy, systems integration, and business process outsourcing. Logica focuses on four market segments, which are Energy and Utilities, Telecom, Finance, Distribution and Transport. Logica strives to deliver custom solutions in order to solve the problems customers face. It is driven to help clients achieve leadership positions and maintain their individual markets. Logica strength lies in the field of industry, domain knowledge, strong managerial and technological knowledge (Logica, 2010).

The research is executed under the program Working Tomorrow in Logica (see Figure 1). This program has been launched to provide students the opportunity to graduate with good command on an innovative coaching. Student can consult with experienced experts in Logica and any innovative ideas from students are welcome. Working Tomorrow enables students to try on their own ideas in practice. Students in Working Tomorrow will be located among five branches of Logica in the Netherlands.

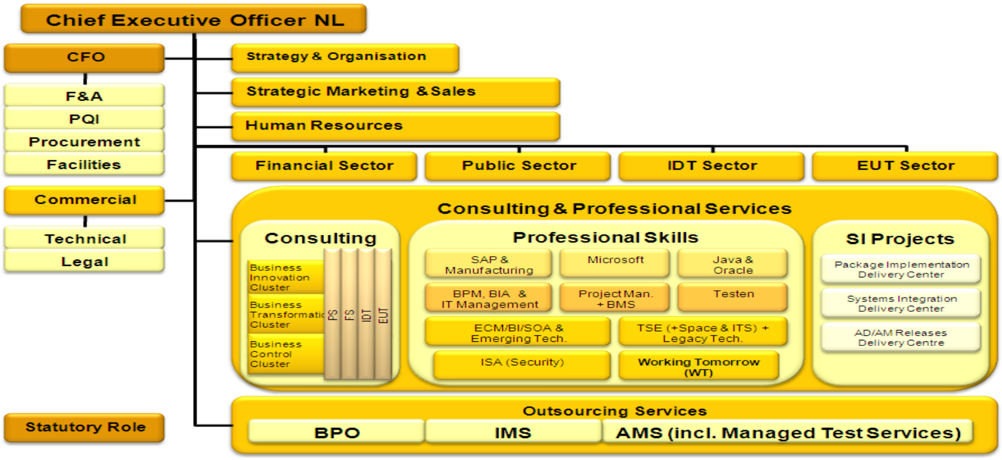


Figure 1 Organization Structure in Logica

1.2 Motivation

Cloud computing is an emerging paradigm ,which provides IT services over a network, shared resources, such as software and storage to customers as a service on demand. It is characterized by its on-demand self-service, rapid elasticity and broad network access(Head, Sailer, Shaikh, & Viswanathan, 2009). Cloud computing has three service models (i.e. Software-as-a-service, Platform-as-a-service, Infrastructure-as-a-service) and four deployment models (i.e. private cloud, public cloud, hybrid cloud and community cloud)(NIST, 2009). The advent of the new technology and its potential advantages enable organizations to deploy and maintain applications more easily and flexibly, reducing the time-to-market and saving cost(Armbrust et al., 2010).

According to one cloud computing adoption survey(Mimecast, 2009), which examines the perception and adoption of cloud computing solutions among 565 IT managers across the US and Canada in the Fall of 2009, 62% of all respondents have considered or are considering cloud computing. Nevertheless, there are still myriads of concerns with regards to cloud computing, including security, privacy, location of cloud services and compliance(Armbrust, et al., 2010; Dillon, Chen, & Chang, 2010).

One of the key disciplines to assist in addressing these challenges and realizing the value of cloud in organizations is governance(Guo, Song, & Song, 2010; O'Neill, 2009b). Cloud governance is the discipline of managing outcomes consistent with measurable preconditions and expectations through structured relationships, procedures and policies applied to the organizations and utilization of distributed capabilities which are under the control of different ownership domains.

In the cloud setting, services would be probably running outside consumer organizations. To some extent, the organizations are sort of losing control over the cloud services. Even though some of the Cloud Service Providers (CSP) offer dashboard for tracking the availability of their services and alerting in a timely manner(ManageEngine, 2011), consumer organizations cannot totally rely on the capabilities to ensure the value of cloud to their businesses. For instance, there are some legal restrictions and business requirements from industry, country or the organizations. How can organizations make sure the compliancy of the services if the services are not under their control? What should the organizations do in the case that the services or the monitoring mechanisms from their providers fail?

The self-service portal from cloud service allows business managers in consumer organizations to bypass their IT departments to subscribe or create any service that suits for their needs. They don’t have to wait a long time for the service delivered by the IT departments. However, the autonomy and flexibility will also bring the organizations to a situation where services and applications are becoming silo again, making the integration difficult. In addition, it is dangerous that if anyone can access, alter or configure the services, especially when more and more cloud services are adopted within the organizations and the dependency of the services become complicated. Without understanding the dependency, changing one service might lead to breaking down another service, even a whole supported business system which is built upon those cloud computing services. It will cause a tremendous business loss and diminish the value of introducing cloud computing at the very beginning(Linthicum, 2009).

The need and importance of having a formal cloud governance regimen is emergent for consumer organizations to ease the transition to cloud computing. The governance regimen can establish an approach for the organizations to reduce risks, maintain business alignment, and maximize of value of cloud computing through a combination of people, process, and technology.

Problems on the cloud governance from the perspective of consumer organizations are summarized in Section in 3.2.1.

1.3 Research objectives and impacts

The research aims at defining a process governance model for assisting consumer organizations to govern their cloud services. Within the governance model, activities and approaches will be identified and specified to help the organizations ease the transition to cloud computing. The research impacts are twofold. First, business managers who are responsible for managing IT resources within their organizations will have a guideline to manage the cloud computing services/assets as well as to align their business needs with the organizations. Managers can rely on this model to figure out the needs to change their organizational structure and introduce new tools to ensure the quality and usage the cloud services. Second, this model can serve as an input for providers to search for new opportunities to develop the governance tools for cloud computing. Besides, they can use this model to analyze their existing capabilities provided to their consumers and to enhance their supporting capability to better cater to the needs of their consumers.

1.4 Research Question

This thesis is guided by the main research question, which is formulated as follows:

How can cloud computing service consumers implement cloud governance within their organizations?

The main research question is refined into the following sub-questions:

1. What are the activities needed to control cloud computing?

   Those activities are the steps which business and IT departments should follow. Those steps will serve as the foundation on which cloud computing governance processes can be built.
2. How can cloud governance be tailored to different types of clouds?

   Cloud computing has different service models and deployment models. The processes might be different regarding the types of cloud. The service models and deployment models are described in Sec. 2.2.
3. What tools can support cloud governance processes?

   Tools can be methodical and help practitioner to create deliverables. Some of the tools can be software tools which can be used to support the deliverables of cloud governance.
4. Should organizations outsource governance?

   This section will discuss whether those tools should be placed in cloud and whether they should be outsourced.
5. How can we test the proposed model?

1.5 Research Approach

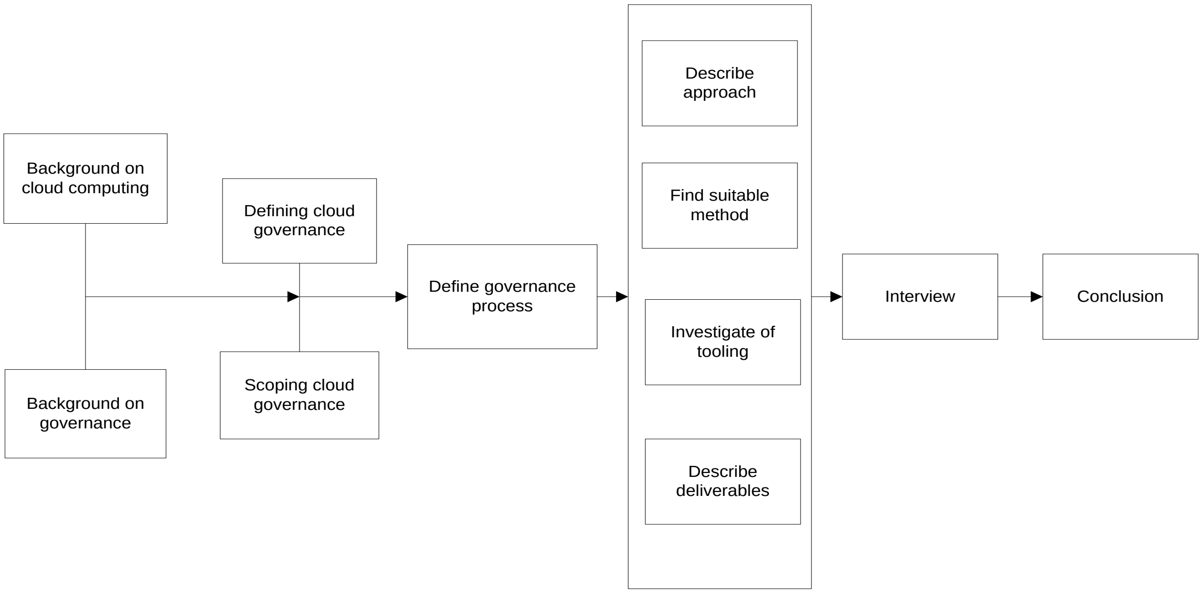


Figure 2 Research Approach

The research is conducted on the basis of the approach described in Figure 2. Firstly, background on cloud computing will be given and it will help understand the state of the art in the realm. Secondly, background on governance will be introduced to help elicit aspects and interest of cloud governance from the perspective of consumer organizations. The scope of cloud governance can be further specified on the basis of problems analysis, cloud governance models and other relevant governance models. Details will be discussed in chapter 3. Thirdly, processes for cloud governance will be specified in line with the domains. After processes are defined, tools, approaches, and deliverables will be identified for each process. Finally a series of interviews from practice will be conducted in order to validate the model.

1.6 Research Focus

Governance can be interpreted to different things. There are some groups studying the cloud governance topic at the moment and the focuses are various. For example, The Cloud Security Alliance (2009) has studied cloud governance from solely security perspective. Our research concentrates on business and IT alignment for cloud governance, which is linked to the problems we have found in literature (see 3.2.1) and the definition we derive from relevant governance literature (see 3.2.2), particularly SOA governance. Detailed governance domains will be discussed in Chapter 3.

The governance subjects are limited to three types of service models and four types of deployment model of cloud computing, which is addressed in chapter 2.

1.7 Report Structure

The structure of the report will be organized as follows:

Chapter 1 this chapter will give introduction and outline of the research.

Chapter 2 this chapter will present the background on cloud computing.

Chapter3 this chapter will cover the background on governance in general, relationship of cloud governance and other governance, and the final scope of cloud governance domains for this research.

Chapter 4 this chapter will present the process governance model for cloud computing; each process in the model will be presented and its corresponding approaches, tools, and deliverables will be discussed.

Chapter 5 this chapter will present the possibilities of implementing governance-as-a-service based on the tools we have identified for those processes.

Chapter 6 this chapter will present the interview and validation results of our proposed model.

Chapter7 this chapter will conclude our research and present further research focus.

2 Cloud Computing

This chapter presents our definition of cloud computing, discusses types of cloud computing which will be used for the governance analysis. Cloud computing is a buzz word confusing most of people in IT filed(Armbrust, et al., 2010). The purpose of this section is not to summarize all the findings regarding cloud computing because that would be an immense work. We only present the information relevant for this research.

This chapter is further structure as follows: section 2.1 presents the definition on cloud computing, Section 2.2 presents the classification of cloud computing, including three types of service model and four types of deployment model. Section 2.3 presents the control levels of cloud computing. Section 2.4 presents the challenges of cloud computing in general from the viewpoint of cloud service consumers.

2.1 Definition of cloud computing

Table 1 provides a holistic view on how researchers define cloud computing. In general, cloud computing is mainly about abstracting IT resources from the underlying hardware and software. These abstract resources are remotely hosted and provided to cloud consumers on demand. Most of the scholars working on cloud computing(Dillon, et al., 2010; Linthicum, 2009) choose the definition from NIST (2009). Nearly other classifications or definitions can be mapped to this definition. Therefore, the definition from NIST has been chosen for our research.

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (NIST, 2009).

From the definition, features of cloud computing can be characterized as follows(NIST, 2009):

- On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed without requiring human interaction with each service's provider.
- Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote being used by heterogeneous thin or thick client platforms (e.g. mobile

phones, laptops, and PDAs).

- Location-independent resource pooling: The provider's computing resources are pooled to serve all consumers using a multitenant model, with different physical and virtual resources dynamically assigned and reassigned according to the consumer demand. The customer generally has no control over or knowledge of the exact location of the provided resources. Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- Rapid elasticity: Capabilities can be rapidly and elastically provisioned to quickly scale up, and rapidly released to quickly scale down. To the consumer, the capabilities available for rent often appear to be infinite and can be purchased in any quantity at any time.
- Measured Service: Cloud Systems automatically control and optimize resource used by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g. storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and the consumer of the utilized service.

(Armbrust, et al., 2010)	"Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. The services themselves have long been referred to as Software as a Service (SaaS), so we use that term. The datacenter hardware and software is what we will call a Cloud"
(NIST, 2009)	"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"
(O'Neill, 2009a)	"An emerging computing paradigm where data and services reside in massively scalable data centers and can be ubiquitously accessed from any connected devices over the Internet. It provides massively scalable power to applications, as well as (in the case of Amazon Elastic Computing Cloud—commonly called Amazon EC2) providing hosting of the applications themselves."

(Wang et al., 2010)	“A computing Cloud is a set of network enabled services, providing scalable, QoS (Quality of Service) guaranteed, normally personalized, inexpensive computing infrastructures on demand, which could be accessed in a simple and pervasive way.”
(Rimal & Choi, 2010)	“The concept of cloud computing represents the converging evolution of distributed computing in terms of infrastructure and application models. The synergistic goal of this computing model is to make a better use of distributed resources, put them together in order to achieve higher throughput and be able to tackle large scale computation problems”.

Table 1 Definitions of cloud computing

2.2 Classification of cloud computing

There are many ways to classify cloud computing. In this paper ,we simply extend the classification from NIST, explaining three service models and four deploy models of cloud computing. And these concepts are also used by most of the literature with regard to cloud computing.

Three service models from NIST are defined as follows(NIST, 2009):

- Cloud Software as a Service (SaaS): The capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
- Cloud Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer controls the applications that run in the environment (and possibly has some control over the hosting environment), but does not control the operating system, hardware or network infrastructure on which they are running. The platform is typically an application framework.
- Cloud Infrastructure as a Service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and

applications. The consumer can control the operating system, storage, deployed applications and possibly networking components such as firewalls and load balancers, but not the cloud infrastructure beneath them.

Four deployment models(Armbrust, et al., 2010; NIST, 2009)

- Public Cloud: In simple terms, public cloud services are characterized as being available to clients from a third party service provider via the Internet. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. The term “public” does not always mean free, even though it can be free or fairly inexpensive to use. A public cloud does not mean that a user’s data is publically visible; public cloud vendors typically provide an access control mechanism for their users. Public clouds provide an elastic, cost effective means to deploy solutions.
- Private Cloud: The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise. It is the internal data center of an organization which is not available to the public.
- Community Cloud: The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premises. Community Cloud can be seen as one type of public cloud while the cost for the type of cloud is more expensive and is more controllable due to the less number of users.
- Hybrid Cloud: A hybrid cloud is a combination of a public and private cloud that interoperates. In this model users typically outsource non critical business information and processing to the public cloud, while keeping business critical services and data in their control.

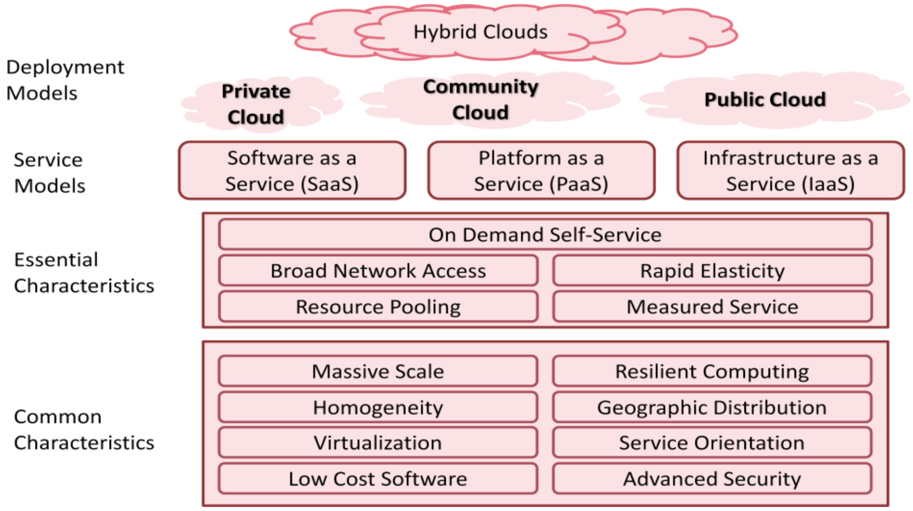


Figure 3 NIST Cloud Definition Framework(NIST, 2009)

2.3 Control of level with regard to cloud types

Traditional IT organizations have to take care of security and control over those five stacks (i.e. Network, Storage, Server, Virtual Machine, and Application). The introduction of cloud disperses the responsibilities between Cloud Service Consumers and Cloud Service Providers. As Figure 4 illustrated, the control level from the consumer side diminishes and the control level from the provider side increases as we move from IaaS to SaaS(Guo, et al., 2010; Rizwan & Lech, 2010). For instance, in IaaS, CSPs offer virtual servers and cloud service consumer has capability to control over the virtual servers and install Operating System (OS) and applications on top of them. However, the infrastructure beneath the virtual server is under the control of CSPs. In SaaS, cloud service consumers can only control the configuration parameters of the services. In PaaS, consumers can control the whole applications while CSPs are responsible for runtime environment and supporting the underlying infrastructure.

When it comes to the public deployment model, cloud service consumers transfer part of the management and control capabilities to CSPs. Nevertheless, it is still contingent for the consumer organizations to adopt some mechanisms to oversee the control capability provided by CSPs. Those mechanisms could be leverage through Service Level Agreement (SLA) management or others.

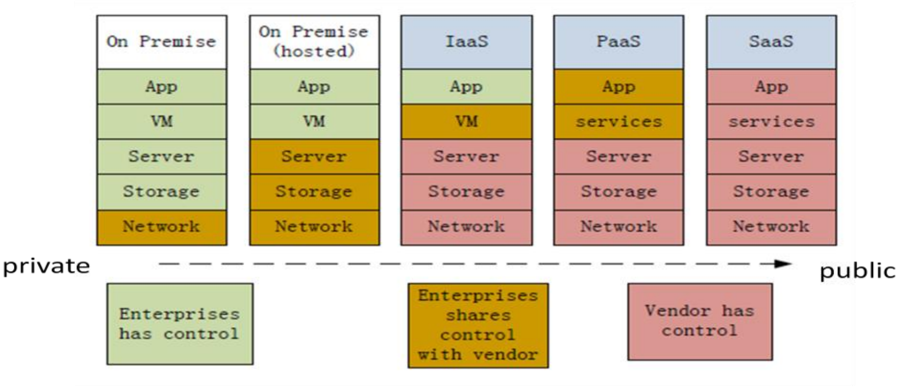


Figure 4 Control Level of Cloud computing (Guo, et al., 2010)

2.4 Challenge of Cloud Computing

The previous graph describes the new paradigm of cloud computing and its potential benefits. However, Consumer organizations also face a lot of challenges brought by the new paradigm According to the survey from IDC (2008), the main challenges regarding the adoption of cloud computing include security, performance, availability, cost efficiency and legal compliance (see Figure 5).

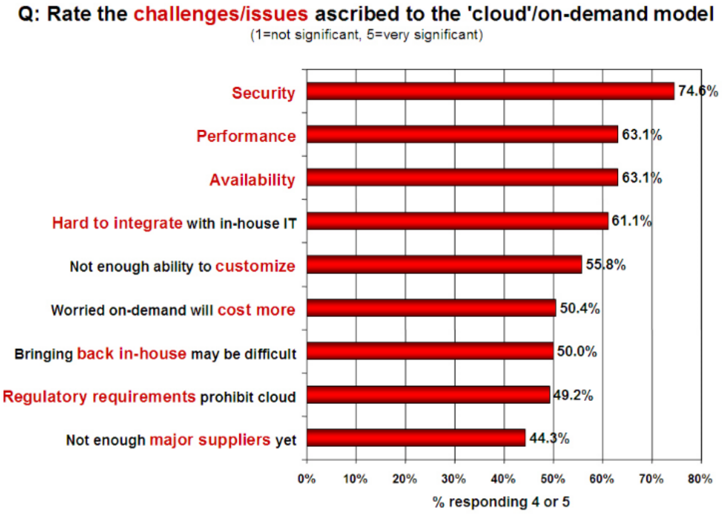


Figure 5 Challenge of adopting cloud computing(IDC, 2008)

3 Cloud Governance

In previous chapter we have presented the basic idea on what cloud computing is and the types of cloud computing. This chapter will focus to answer what cloud governance is and to define governance domains for our model.

This chapter is further structured as follows: Section 3.1 presents relevant governance background. Section 3.2 defines cloud governance for this research. The definition of the cloud governance is based on the problems analysis of cloud governance from relevant literature, relevant governance background presented in Section 3.1 and the existing definitions of cloud governance. Section 3.3 presents existing models used for designing our own model.

3.1 Background on Governance

3.1.1 Corporate Governance

Corporate Governance is defined as "the set of processes, customs, policies, laws and institutions affecting the way in which a corporation is directed, administered or controlled" (de Leusse, Dimitrakos, & Brossard, 2009)**.** It addresses the need for a mechanism to ensure that there is compliance with the laws, policies, standards and procedures under which an organization operates. Governance is about

- Establishing chains of responsibilities, authority and communication to empower people (decision right).
- Establishing measurement, policy and control mechanisms to enable people to carry out their roles and responsibilities.

Corporate governance covers every aspect of businesses ranging from human resource department to purchasing and marketing.

3.1.2 IT Governance

IT Governance includes the decision rights, accountability framework and processes to encourage desirable behavior in the use of IT(COBIT, 2005). By definition, IT governance can be treated as part of corporate governance which pertains to Information Technology processes and supports the goal of business. It emphasizes the management and control of IT assets, people, processes and infrastructures as well as the way in which the assets are managed and procured.

The IT Governance Institute adopts a more extensive definition, which suits better to the scope of this thesis: “IT governance (…) is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization’s IT sustains and extends the organization’s strategies and objectives.”From this definition it appears that IT governance is responsible for aligning business strategy with IT, as well as “extending” this strategy in order to achieve the business value. The IT Governance Institute distinguishes the following four focus areas in IT governance, the first two are related to business value, the second two are related to compliance:

- Performance measurement
- IT value delivery
- IT Strategic alignment
- Risk management

3.1.3 SOA governance

Service Oriented Architecture (SOA) governance has been selected because currently most of the researches mention that SOA governance technologies and methods can be leveraged for cloud setting (de Leusse, et al., 2009; Linthicum, 2009; O'Neill, 2009b).

SOA governance is an extension of IT governance(Keen et al., 2007; The_Open_Group, 2009), which, in turn, is an extension of corporate governance. SOA governance makes changes from IT governance to ensure that the concepts and principles for service orientation architecture are managed appropriately and that services are able to deliver in line with the business goals.

Core problems of SOA governance from business and IT alignment perspectives include (Linthicum, 2009; Nadhan, 2004; Progress_Software, 2005; Schepers, 2007):

- Hard to assure compliance to regulations and legislation: it is emergent to have audit trail IT system to audit behavior of the services.
- Hard to create budget for the services within an organization since the services are cross organizational units.
- Hard to control consequences of changing services due to various consumers of one service and the unclear dependencies of different services.
- Hard to guarantee quality of services: service qualities have to make sure to be compliant to the laws and regulations during design time and ensure quality of services can be met during run-time ,especially the performance of services.

- Hard to ensure the created services can correctly address the business value and needs.

In accordance with the problems addressed above, most of SOA governances from both practice and literature concentrate on the follows aspects(IBM, 2011a; webMethods, 2006):

- Service Governance: it mainly refers to service lifecycle management and establishing decision rights for the development, deployment, operation and management of new services.
- Organizational change: it refers to defining responsibilities on who should monitor as well as report decisions and results for communication.
- Make sure the services are aligned with business goals and value.

Since SOA governance itself is a big topic while the focus of the thesis is not about SOA governance. We will address some of the relevant SOA governance models as a guideline in order to define our own model. More detailed governance aspects relevant for cloud governance from those SOA governance models will be discussed after we provide our definition for cloud governance.

3.1.4 Comparison

Corporate governance focuses on setting processes, roles, and policies in line with business to ensure that business goals have achieved. IT governance concentrates on IT decisions and policies to ensure IT implementation to meet business goals. SOA governance is part of corporate governance that deals with regulating and monitoring the components from service-oriented architecture. It also encompasses the decisions on services which realize and accomplish IT governance goals. Therefore we summarize the relationship of different governances mentioned before in Figure 6.

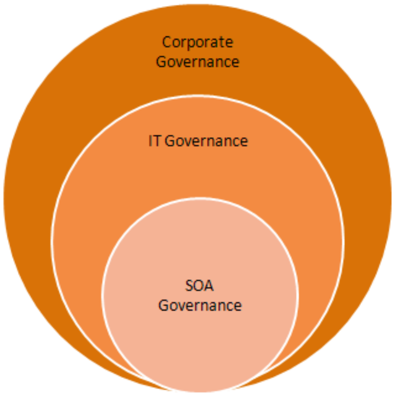


Figure 6 Relationship of different governances

3.2 Introduction on Cloud Governance

This section will concentrate on cloud governance. We will first collect the problems of governing cloud computing from literatures. Problems we have collected are mainly from business and IT alignment perspective. The relevancy of the business/IT perspective is base on the background we have discussed in previous sections. The definition of cloud governance will be given in line with our research objectives. Finally, positioning of cloud services is discussed, in which the relationship of cloud and SOA is presented. This serves as an important input for outlining the domains of cloud governance.

3.2.1 Cloud Governance Problem Analysis

Problems regarding cloud governance have been summarized in Appendix B. Along with each category, a description for the category is given. Several repeated problems mentioned in the literature (Bentley, 2010; Binning, 2009; Cheliah, 2011; Dinoor, 2010; Guo, et al., 2010; Hollis, 2011; Linthicum, 2009; ManageEngine, 2011; Menken & Blokdijki, 2009; Microsoft, 2010; Vael, 2010)include:

- Compliance to laws and standards
- Consequences of changing services
- Ensuring quality of the services
- Aligning organizations with the cloud
- Cooperate with suppliers and evaluate suppliers and their services

Compliance to laws and standards can be solved by carefully observing/conducting risk assessment before establishing the project. Some of the compliance issues, consequences of changing services and ensuring quality of the services are related to service behavior as a whole. The service behavior can be guaranteed through defining policies, monitoring the execution of the services, and creating criteria to develop services. Aligning organizations with the cloud can rely on creating new adoption approaches for cloud, establishing new funding models to charge the services, and introducing new units and roles to be in charge of cloud services. Cooperating with suppliers can be ensured through agreeing upon the communication schemes and service level agreement items. Finally, evaluating suppliers can rely on the monitoring reports and business goals achieved through the services from suppliers.

In order to resolve those problems better, we need to find a suitable structure to organize the solution areas. The solution areas or phrases will be identified based on the existing governance models from cloud governance field or similar fields. Relevant researches are conducted in the following sections.

3.2.2 Definition of Cloud Governance

Cloud governance is a new term in IT field. There has not been a definition published by any official organization yet. According to CTO of Vordel(O'Neill, 2009b), Cloud governance involves “applying policies to the use of cloud services”. Cloud Computing Use Discussion Group (2010) shares the same idea that cloud governance is about “the controls and processes that make sure policies are enforced”. Correspondingly, Guo et.al (2010) defines governance in cloud as “the processes used to oversee and control the adoption and implementation of cloud-based services in accordance with recognized policies, audit procedures and management policies”. Similarly, Microsoft (2010) defines cloud governance as “defining policies around managing the above factors [availability, security, privacy, location of cloud services and compliance etc.] and tracking/enforcing the policies at run time when the applications are running”. According to those definitions, defining policies is important, but defining processes to enforce those policies is also essential for accurately enforcing the policies.

Concept of “governance” in cloud can be derived from corporate governance and IT governance. What is missing from most for the definitions of cloud governance is about contribution of cloud governance to achieving business goals. Besides, most of the definitions do not explicate relationship management. For instance, relationship management with cloud service providers. Governance of cloud is more than policy management and defining processes to ensure that policies have been correctly enforced. Comparing to those definitions, the definition set by Agilepath_Corporation (2011) outlines the importance of alignment cloud with business goals. Cloud governance has to support business strategy and ensure service value, service quality and security regardless the control and locations of the services. For our research we define cloud governance as:

Cloud governance is a framework for the leadership, organizational structures and business processes, standards and compliance to these standards, which ensure that the organization’s cloud capability supports and enables the achievement of its strategies and objectives.

Therefore, a comprehensive cloud governance model should contain at least three main aspects:

- “Processes”- outline the processes to introduce cloud computing within organizations.
- “Organizational structures”- adjust current organizational structure, roles and responsibilities to ensure better support of implementing cloud computing and governance.
- “Enabling Technologies” – introduce new tools and infrastructure to enforce the governance capabilities.

3.2.3 Position of Cloud Governance

In previous sections, we have presented the problems with which cloud governance confronts and the definition of cloud governance used in this research. This section is going to discuss what's new for cloud governance and from what we can derive our cloud governance model.

When analyzing and summarizing the problems for cloud governance, we have found that the problems on cloud governance resemble the problems of SOA governance mentioned in 3.1.3. According to the literature(Agilepath_Corporation, 2011; Linthicum, 2009), most of cloud services are designed in line with the SOA principles, cloud computing can be treated as one of the implementation and realization approaches for SOA(See Table 3). At the mean time, SOA as well as virtualization technology, realize the "resource pooling" characteristic from cloud. Both of SOA governance and cloud governance require enterprise-wise cooperation (e.g. communication between IT and Lines of business) to realize the business value. Therefore, governance related to SOA governance, such as service governance and organizational change, is the most applicable approaches to cloud computing. It is easier to leverage SOA governance approaches to cloud servicers governance (Linthicum, 2009).

However, cloud governance do not equal to SOA, there are some differences between them. For instance, cloud computing emphasizes pay-as-you go business model while SOA does not. Detailed similarities and differences between them have been summarized in Table 2.

Similarity:

- Organization-wise management: require moving away from local divisions or departments to issues to prioritize usage based on overall the business requirements(Ovum, 2010).
- The core of SOA and Cloud governance are service governance, for instance , lifecycle management of service , design time , runtime and change time of management (Linthicum, 2009; O'Neill, 2009b).
- Require a new cost allocation/funding model for service within an organization (Australian_Government, 2011; Bentley, 2010).
- Process-oriented: both cloud governance and SOA governance should rely on processes to increase the awareness of stakeholders for proper usage rather than merely rely on governance tools(O'Neill, 2009b).
- Dependency management: cloud computing requires organizations to keep up with integrated, portable, abstracted and open IT asset. The more assets have been introduced, the more

dependencies are needed to manage(Ovum, 2010).

- Rely on policies to ensure the right behavior of services, the focus moves from coding software components to defining the purpose via contact details and capability information in the context of policies (Peterson, 2010; van de Dobbelsteen, 2007).

Differences:

- Cloud governance technologies demand federation capabilities to synchronize both internal and external cloud registry/repositories. Even though SOA aims for Business to Business services and integration, current governance tools for SOA are still lack of the synchronization capability with external registry/repositories. More investigation on the SOA governance tools is needed to be adaptive to the cloud setting (DevCentral, 2008; Guo, et al., 2010; Linthicum, 2009; Open_Cloud_Standards_Incubator, 2010).
- Abstraction is one of the features of cloud computing, this is particular for public cloud where services are deployed outside the boundary of the organization. The problems raised by abstraction could include remote service testing and interface versioning change etc.(Hurley, 2010; King & Ganti, 2010).
- SLA (Service Level Agreement) management is much more important in cloud context because services , particularly public services, are running out the organization, requiring an delicate contract to ensure the quality of services for their business (Australian_Government, 2011; Grobauer & Schreck, 2010).
- Cloud computing emphasizes on scalability, high performance[1] (e.g. resource pooling) and multi-tenant while SOA does not (Yi & Blake, 2010).
- Policy management in cloud computing is more complicated in cloud setting because not all the services running in cloud can enforce the policies set by consumer organizations. Sometimes policies are under the control of providers and consumer organizations need to manage both internal policies and public policies (Ovum, 2010).
- SOA emphasizes on managing assets first, enforcement and monitoring second. In contrast, cloud demands organizations to address enforcement and monitoring first(Layer7, 2011).

Table 2 Similarity and differences of cloud governance and SOA governance

SOA	Cloud computing
The platform service (Service-Oriented	IaaS and PaaS have been designed on the basis of

[1] Automated scalability is not necessarily provided by cloud CSP

Infrastructure): delivers the hardware and software foundation such as server, network, database, operating system, clustering/grid/virtualization etc. on which software components run but are abstracted from.	SOA principles.
The application/process service level: refers to software-only services.	Many SaaS applications have been designed on the basis of SOA principles.

Table 3 Mapping service level of cloud computing and SOA(Ovum, 2010)

Cloud governance is one of sub-branches in IT governance, through controlling the usage of cloud services, a specific type of IT services, in order to deliver the value to support business needs. A more specific relationship for cloud governance is its link to SOA governance. The overlap and similarities between cloud computing and SOA provide us an indication to sketch a cloud governance model on the basis of exiting SOA governance models as well as cloud governance literatures. Figure 7 summarizes the relationship between cloud governance and other governances we mentioned before.

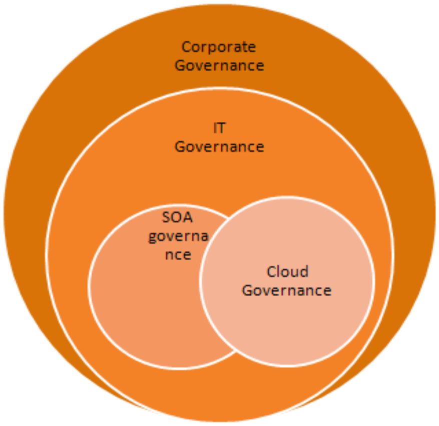


Figure 7 Position of Cloud Governance

3.3 Existing Governance Model

Creating a structured solution requires a more specific solution bundles in order to cope with the problems we have found in 3.1.3. The position of cloud governance in previous section suggests that SOA governance solution bundles will be applicable to cloud as well. Another useful input for structuring the solution bundles include existing cloud governance frameworks or models. This section will introduce the relevant models. The purpose to present those models is twofold. On the one hand, those models can be served as very important inputs to define our solution bundles. On the other hand, we can find a suitable reference for our process modeling.

3.3.1 Schepers' Lifecycle SOA governance Model

Schepers (2007) has developed a lifecycle approach for SOA governance. The governance areas from his model include portfolio governance, technology governance, project governance and service level governance. This model consists of six phrases to monitor SOA within an organization. Creating a SOA strategy is the task which triggers the whole model and its processes. The lifecycle shows the order in which the phases should be initiated. However, the order does not imply that a chronological order between the phrases. For each process, relevant approaches/tooling and outputs of the process are discussed. The six areas have been summarizes as follows(Schepers, 2007):

- SOA strategy (vision): this phrase contains the long-term planning on SOA, funding models and involvement of stakeholders.
- Organizational alignment to SOA (plan): this phrase concentrates on the organizational changes and roles/responsibilities adjustment for better business/IT alignment. For example, creating excellent of centre for knowledge sharing.
- Portfolio management (design): this phrase is about establishing processes to determine which service to create and when to add one service to the portfolio.
- Service lifecycle management (build): this phrase is about ensuring qualitative service development and launching change management.
- Policy management (deliver): this phrase concerns about how the service quality can be guaranteed.
- Service level management (operate) is about the operational quality of SOA services.

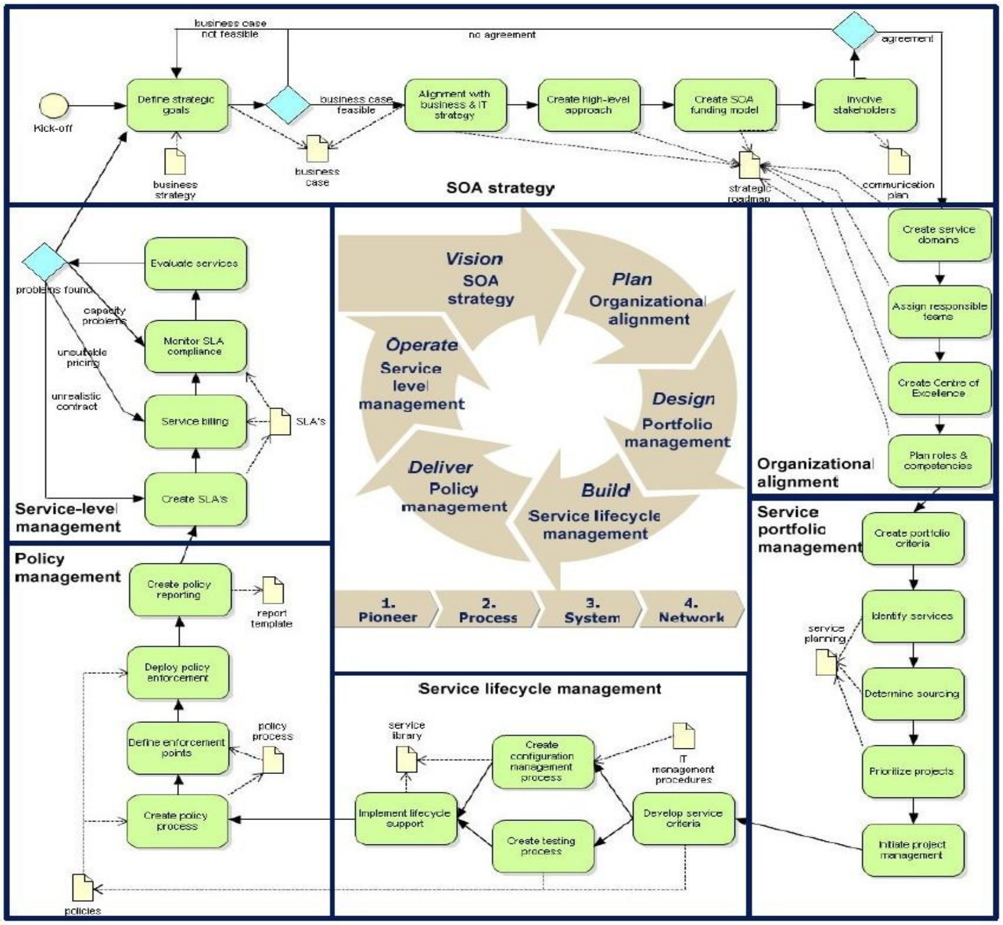
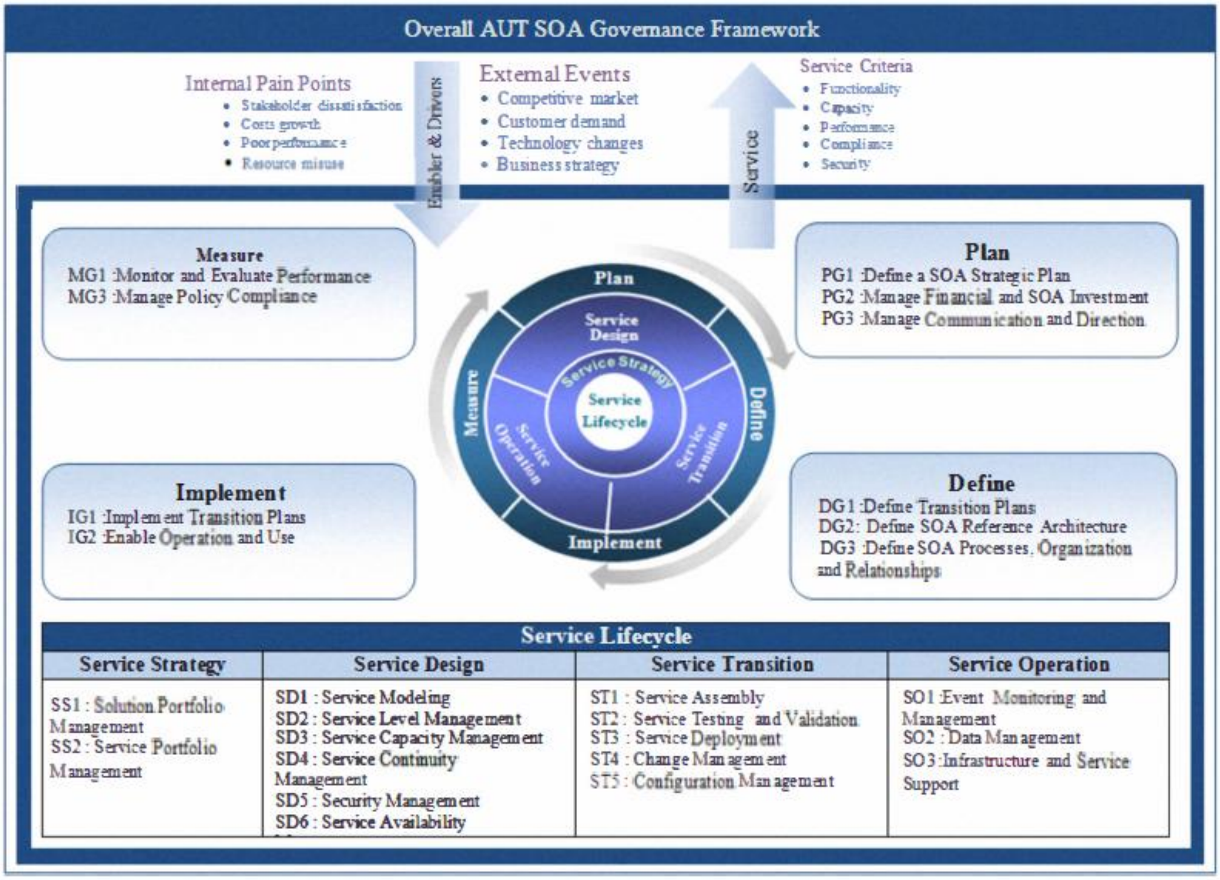


Figure 8 Lifecycle Method for SOA governance (Schepers, 2007)

3.3.2 AUT SOA Governance Framework

Another SOA governance framework which has been chosen is from Hojaji and Shirazi (2010). This framework is obtained by enforcing governance structures of COBIT and thorough analysis of six existing popular SOA governance models, including ORACLE, webMethods (2006), IBM(Brown, Moore, & Tegan, 2006),Bieberstein(Bieberstein, Bose, Fiammante, Jones, & Shah, 2005), CBDI-SAE(CBDI, 2008), and Software AG(Castaldini, 2008). It applies service management activities into a lifecycle approach. This framework offers a well-defined, structured set of processes. This model is included such that it can be complementary to the model from Schepers in order to provide other solution bundles for cloud governance when it is necessary.


Overall AUT SOA Governance Framework
Internal Pain Points
Stakeholder dissatisfaction
Costs growth
Poor performance
Resource misuse
Enabler & Drivers
External Events
Competitive market
Customer demand
Technology changes
Business strategy
Service
Service Criteria
Functionality
Capacity
Performance
Compliance
Security
Measure
MG1 :Monitor and Evaluate Performance
MG3 :Manage Policy Compliance
Plan
PG1 :Define a SOA Strategic Plan
PG2 :Manage Financial and SOA Investment
PG3 :Manage Communication and Direction
Plan
Service Design
Service Strategy
Service Lifecycle
Measure
Service Operation
Define
Service Transition
Implement
Implement
IG1 :Implement Transition Plans
IG2 :Enable Operation and Use
Define
DG1 :Define Transition Plans
DG2: Define SOA Reference Architecture
DG3 :Define SOA Processes, Organization and Relationships

Service Lifecycle

Service Strategy	Service Design	Service Transition	Service Operation
SS1 : Solution Portfolio Management SS2 : Service Portfolio Management	SD1 : Service Modeling SD2 : Service Level Management SD3 : Service Capacity Management SD4 : Service Continuity Management SD5 : Security Management SD6 : Service Availability	ST1 : Service Assembly ST2 : Service Testing and Validation ST3 : Service Deployment ST4 : Change Management ST5 : Configuration Management	SO1 :Event Monitoring and Management SO2 : Data Management SO3 :Infrastructure and Service Support

Figure 9 AUT SOA Governance Framework (Hojaji & Shirazi, 2010)

3.3.3 Guo's Cloud Governance Model

Guo et.al. (2010) introduces a governance model for cloud computing. This model is the only one in academic field discussing aspects of cloud governance in general. There are some other researches reporting the cloud governance, which focuses on security aspects(Cloud_Security_Alliance, 2009) and resource provision(Litoiu & Litoiu.M., 2010). These researches are not useful for articulating solution bundles to solve all the problems we state above. Compared with the previous models from SOA, this model does not initiate from the business strategy and it neglects the organizational alignment, roles and responsibilities adjustment. This model outlines the necessary components for cloud governance and concentrates on policy modeling, operational model and other management activities such as service management, risk management, security management and policy management. However, the gap between IT and organizational alignment will probably lead to devalue the introduction of cloud computing.

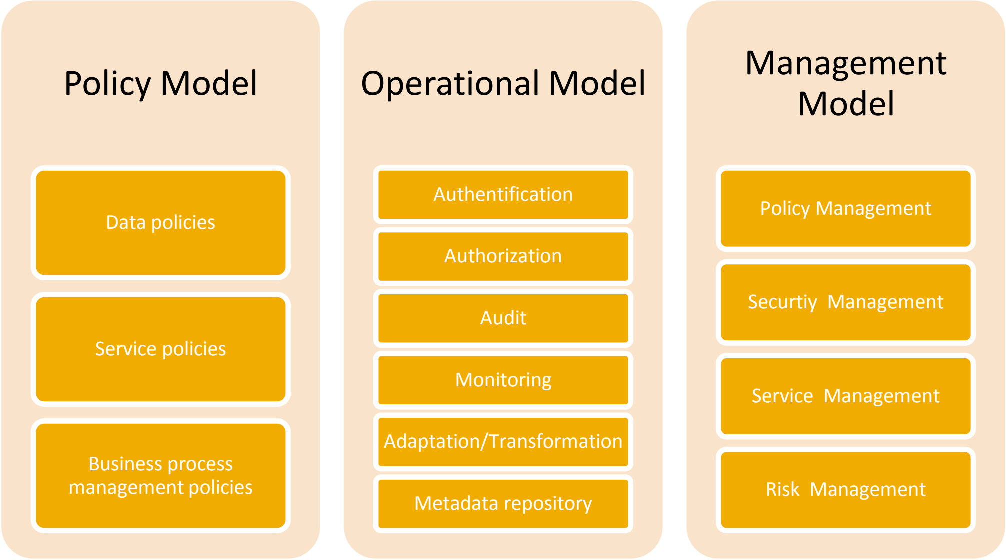


Figure 10 Cloud Governance Model from Guo et al. (Guo, et al., 2010)

3.3.4 Microsoft's Cloud Governance Model

Microsoft (2010) also proposes a cloud governance model for its azure cloud platform. The main focus of the governance model from Microsoft is about policy management. The model is composed of three main parts, including design time, run time governance and change management governance. During design time, it is imperative to define service policies, quality of standards and SLA levels. During runtime, policies are enforced and the application/service performance and compliance are carefully monitored. Change management governance is set to track the change activities and asset. It is required to provide and manage report, alert, and log at the same time. The three components work together to ensure correct versioning, scale and ensure security compliance. This model is similar to Guo's model, outlining key components of cloud governance but omitting the activities which address the alignment of IT and business.

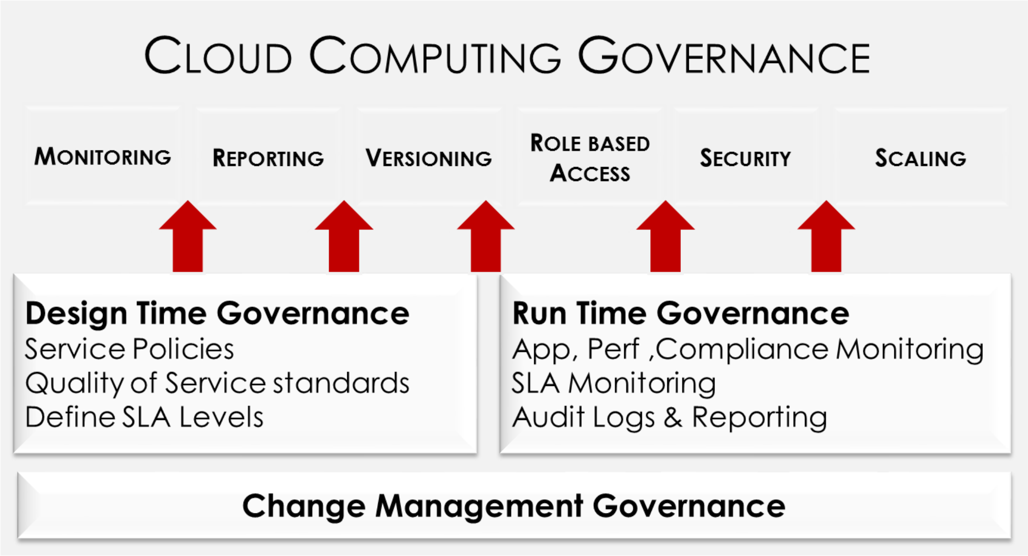


Figure 11 Microsoft's Cloud Governance Model(Microsoft, 2010)

3.3.5 Comparative Analysis

This section will conduct a small comparative analysis among the models mentioned above. In order to have a suitable analysis, we define several criteria for the evaluation, which are summarized as follows:

- High coverage of problems addressed in 3.1.3: the proposed model should cover the problems we have identified in 3.1.3 as much as possible.
- Parsimonious: the proposed model should not be complicated so that organizations can follow the methodology easily. The model can be refined later as more experience has been gained from the practice. What we define "parsimonious" is that it should not contain too many items within the model. The model should be understandable and the structure of the model should be logical and reasonable.
- Process-oriented: This criterion is derived from the definition we have given.
- Lifecycle approach: lifecycle approach demands that the model should include a feedback loop. This will help to emphasize that governance of cloud is an on-going, dynamic process instead of one-time work. As organizations get more mature, and more feedback is collected, it will require the organizations to go through those processes and adjust some of the processes if necessary.
- Applicability of solution: discuss whether the detailed solution can be directly applied to the cloud situation.

Models Criteria	Schepers' model	AUT SOA model	Guo's model	Microsoft
Coverage of problems	All	All	Partially	Partially
Parsimonious	Yes	No	Yes	Yes
Process Oriented	Yes	Yes	No	No
Lifecycle approach	Yes	Yes	No	No
Applicability of Solution	Partially	Partially	Yes	Yes

Table 4 Comparative analysis

In the Schepers' model, compliance to laws is ensured through policy management and SLA monitoring during run-time. Service behavior (e.g. service dependency, changing of service) can be ensured by SLA management and service lifecycle management. Aligning organizations with the cloud is ensured through organizational alignment and SOA strategy. Cooperation with suppliers and evaluating services are ensured through SLA management.

In the AUT SOA model, compliance to laws is guaranteed through "manage policy compliance" in the measurement phrase. Service behavior is guaranteed through "Service lifecycle" phrase. Aligning organizations with the cloud is guaranteed through "Plan" and "Define" phrase, in which a set of plans and processes within the organizations have been created or adjusted. Cooperation with suppliers is guaranteed through "Service Level Management" in the Service Lifecycle phrase and "monitoring and evaluate performance" in Implement phrase.

The solution areas from these two SOA governance models cover all the problems we have identified in 3.1.3. However, the solution areas from Microsoft and Guo's model, as we have mentioned in 3.3.3 and 3.3.4, mainly focus on policy management and SLA management. Both models are missing relevant assessment and adjustment on organizational structure and roles in order to make sure better business and IT alignment.

Speaking of the complexity of the models, Schepers' model, Microsoft and Guo's model are well defined according to their defining requirements. However, the model from AUT is more complicated since it includes too many processes in the model. Relationships between the inputs/outputs and the processes are not well defined in AUT model.

Two SOA governance models are clearly process-oriented and apply the lifecycle methodology in their models. However, the process-oriented feature in the two cloud governance models is not so obvious. In Guo's model, there are some processes in its management component. In Microsoft's model, some part of the model can be treated as process-oriented such as define SLA and monitor SLA. We cannot find any lifecycle approach within Guo's and Microsoft's model.

As SOA governance is designed for cloud and we have discussed the similarity and differences in Table 2, the solutions and detailed tools from SOA cannot directly apply to the cloud.

The final evaluation results for all the models are presented in Table 4. According to the results, the Schepers' model can be chosen as a reference model to define the final solution bundles and the processes of our cloud governance model. As discussed before, the solutions approaches and tools from SOA cannot totally be applied to cloud, we have to rely on some literatures on cloud computing when discussing and defining the cloud model.

4 A Lifecycle Process Model for Cloud Computing

Previous chapters have analyzed the problems of cloud governance and selected the Schepers' SOA model as the reference model for our process modeling. This chapter will continue to define and analyze the final domains of our process model for cloud computing on the basis of the reference model and corresponding literature reviews.

This chapter is further structured as follows: Section 4.1 will present the process model as whole, within which the final domains for the model will be discussed and a template used for process analysis will be presented. Section 4.2 to 4.6 will describe each process in detail from those five domains according to the template.

4.1 Introduction of the Process Model

The Schepers´ SOA model focuses on six aspects (i.e. SOA strategy, organizational alignment, portfolio management, service lifecycle management, policy management, and service level management). The six domains fit into the Enterprise-Value-Delivery framework from Deloitte(Delioitte, 2006). Based on these six domains, we collect literature on those aspects and find out that cloud governance aspects could basically be covered by these six aspects. Final domains of our cloud process governance model have compacted into five domains, following the lifecycle of vision, define, deliver, build and operate (see Figure 12). The portfolio management section from Schepers' model has been removed and the two processes within this domain have moved to strategic plan because service selection and determine delivery model should belong to visioning when one organization decides to move to cloud. In addition, cloud service identification and delivery model determination will rely on workload requirements besides business requirements (e.g. security requirement).Thus it is necessary to discuss the activities and methods regarding those two processes. Other portfolio management activities such as prioritize projects will be the same as traditional service portfolio management and are out of the scope of this thesis. Therefore, a final description with respect to the five domains is summarized as follows and a further summary on those five domains can be found in Appendix C.

- Strategic planning (Vision): this domain concerns about high level strategic determination, including setting up Key Performance Indicators to realize business goal, involving with stakeholders and defining methodology to choose service model and deployment model.

- Organizational alignment (Define): this domain concerns about organizational change such as introducing new units for cloud computing knowledge management and facilitating cloud adoption within an organization, ensuring existing role competency for cloud service management and establishing funding capability to support cloud service cost allocation within the organization.
- Service Lifecycle Management (Build): this domain concerns about creating services using cloud platform and resources. What types of criteria organizations should follow when creating a service on top of cloud and how they make sure the service quality during the design time (e.g. testing cloud service) will be discussed in this domain. Moreover, tools used to manage cloud service lifecycle management will be analyzed, which will support interface versioning and authorization.
- Policy Management (Deliver): this domain concerns about policy management and enforcement regarding cloud services. Policy management focuses on internal policy management processes and external policy mapping with the policies from public CSPs. Run-time policy enforcement tools from SOA will be extended for cloud services and corresponding policy reports will be used for monitoring and improvement.
- SLA Management (Operate): this domain concerns about quality of services and metrics used to evaluate and monitor the performance of services. Monitoring and ensuring that the SLA can be met is one of the main concentrations for cloud governance, especially for public cloud.

Figure 13 offers a holistic view on the whole process model for cloud governance. The highlighted steps include specific characteristics regarding cloud services. Either the activities within the process are influenced or the tools used to support the activities have new functions and requirements in the cloud. The deliverables of each process in the model have not been totally matched to detailed processes since outputs of each process are different and it is difficult to present them all in one figure. Audiences can find the detailed outputs from the process discussion section, where a template will be used. We try to generalize common processes regardless of the types of cloud; however, there are some differences among several processes due to different control levels. We have summarized the relationship between processes and types of cloud in Appendix G.

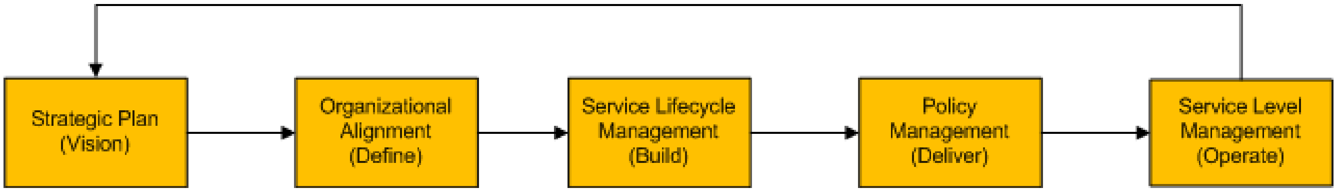

Strategic Plan (Vision)
Organizational Alignment (Define)
Service Lifecycle Management (Build)
Policy Management (Deliver)
Service Level Management (Operate)

Figure 12 High Level Process for cloud governance

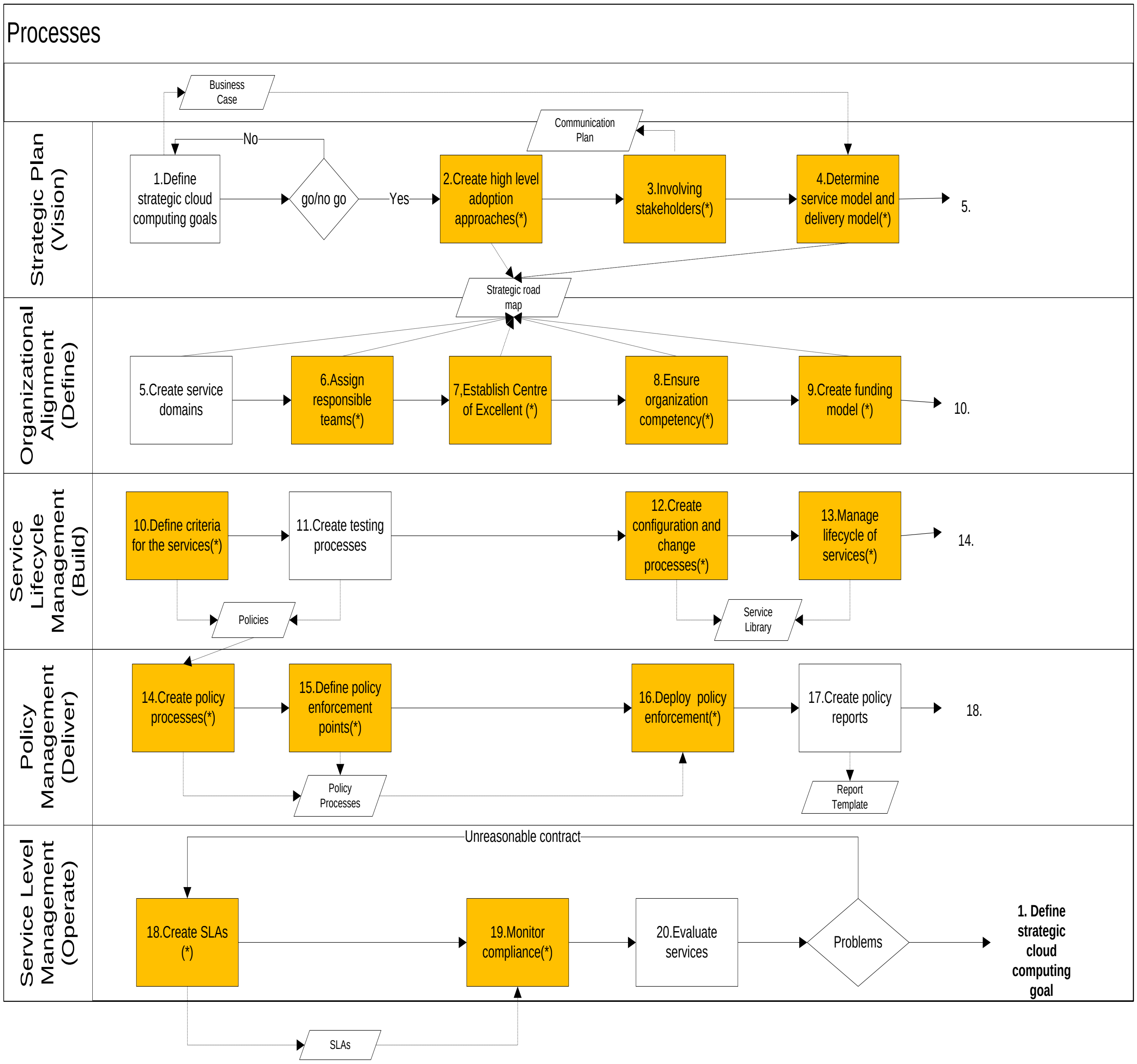

Processes
Business Case
Communication Plan
Strategic Plan (Vision)
1.Define strategic cloud computing goals
No
go/no go
Yes
2.Create high level adoption approaches(*)
3.Involving stakeholders(*)
4.Determine service model and delivery model(*)
5.
Strategic road map
Organizational Alignment (Define)
5.Create service domains
6.Assign responsible teams(*)
7,Establish Centre of Excellent (*)
8.Ensure organization competency(*)
9.Create funding model (*)
10.
Service Lifecycle Management (Build)
10.Define criteria for the services(*)
11.Create testing processes
12.Create configuration and change processes(*)
13.Manage lifecycle of services(*)
14.
Policies
Service Library
Policy Management (Deliver)
14.Create policy processes(*)
15.Define policy enforcement points(*)
16.Deploy policy enforcement(*)
17.Create policy reports
18.
Policy Processes
Report Template
Service Level Management (Operate)
Unreasonable contract
18.Create SLAs (*)
19.Monitor compliance(*)
20.Evaluate services
Problems
1. Define strategic cloud computing goal
SLAs

Figure 13 Low Level process and overview on the delivery of each process

Template for process discussion

In order to make the discussion more structural, we have introduced a template for each process discussion, including process name, description, method and deliverable. Detailed descriptions regarding each component are shown in Table 5.

Process Name	Name of the process
Description	• Describe generic goals of the process. • Articulate problems that can be solved in the process. The problems will be related to the features of cloud computing. (optional) • Present related work from SOA, which can be refined into cloud setting (optional).
Method	• Describe tools used to support the process. If there are no standard tools available, some of the requirements for the tools will be outlined.
Deliverable	• Describe deliverables of the process and present requirements for the deliverables such as what should be included in a SLA template.

Table 5 Description on process discussion template

4.2 Strategic Plan

This section will concentrate on creating high level cloud computing vision. Introduction of cloud computing is analogous to other IT services, requiring to align business needs so as to ensure the value of the service for the organization. High level vision is the first step for proper governance of cloud service. Strategic plan will tackle the following questions: what goal should be achieved? How is cloud service coordinated? How will an organization choose a service? Processes for this section are identified from the reference model (see Figure 14). Detailed discussion will follow the template described in 4.1.

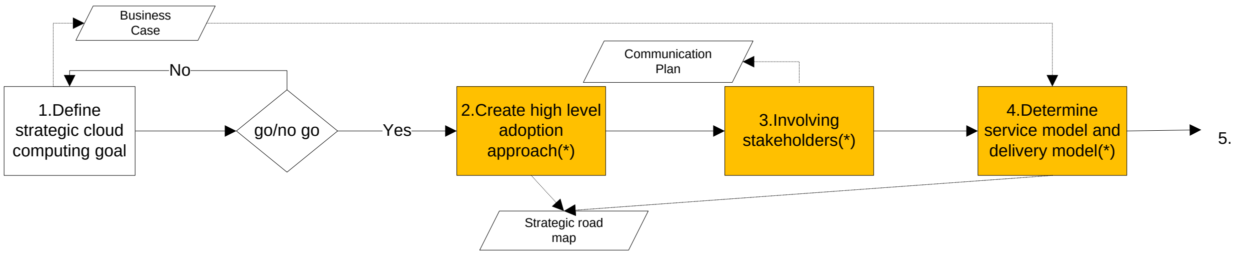
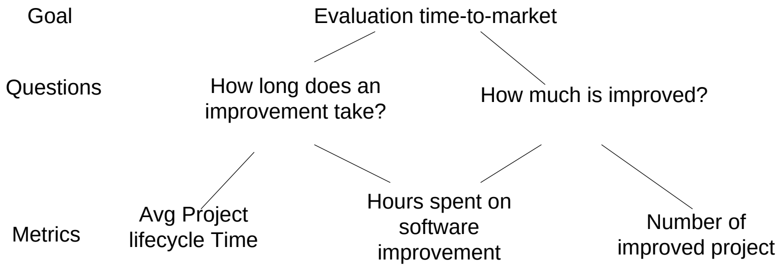

Business Case
No
Communication Plan
1.Define strategic cloud computing goal
go/no go
Yes
2.Create high level adoption approach(*)
3.Involving stakeholders(*)
4.Determine service model and delivery model(*)
5.
Strategic road map

Figure 14 Strategic Plan

4.2.1 Define strategic cloud computing goals

Process Name	**Define strategic cloud computing goals**
Description	Cloud governance should connect to high level business strategy and present an argumentation why business needs can be realized by introducing cloud computing(Ovum, 2010). Organizations should not introduce cloud computing only because it is a new technology. Instead, cloud computing should be used as a mean to achieve business goals. Creating a business case can be considered as a normal way to ensure the reasons to adopt cloud computing services(Linthicum, 2009). The business goals should be measurable so that the organization can manage in a more tangible way. In order to make sure successful alignment, it is necessary to transfer the business goals into high level key performance indicators(Schepers, 2007). More detailed KPIs can be refined during the following strategic execution. KPIs can be an important input for a business case because of the measureable initiatives. Creating business cases will become easier when KPIs can be translated into financial benefits(IBM, 2010b; Linthicum, 2009; Marks & Lozano, 2010). Return of Investment (ROI) and "Goal-Question-Metric" proposed by Schepers(2007) can be still applied to this translation initiative for cloud(Bentley, 2010; Creswich, 2010).
Method	**Goal-Question-Metric (GQM)** Goal question metric is an approach from software engineering used to break down some vague concepts into measurable metrics. Several questions are derived from the goals which need to meet with business needs. The questions can be continuously broken down into smaller manageable questions. Then metrics are identified in order to answer those sub-questions (see the following example).  Goal Evaluation time-to-market Questions How long does an improvement take? How much is improved? Metrics Avg Project lifecycle Time Hours spent on software improvement Number of improved project Figure 15 Example of GQM(Schepers, 2007)

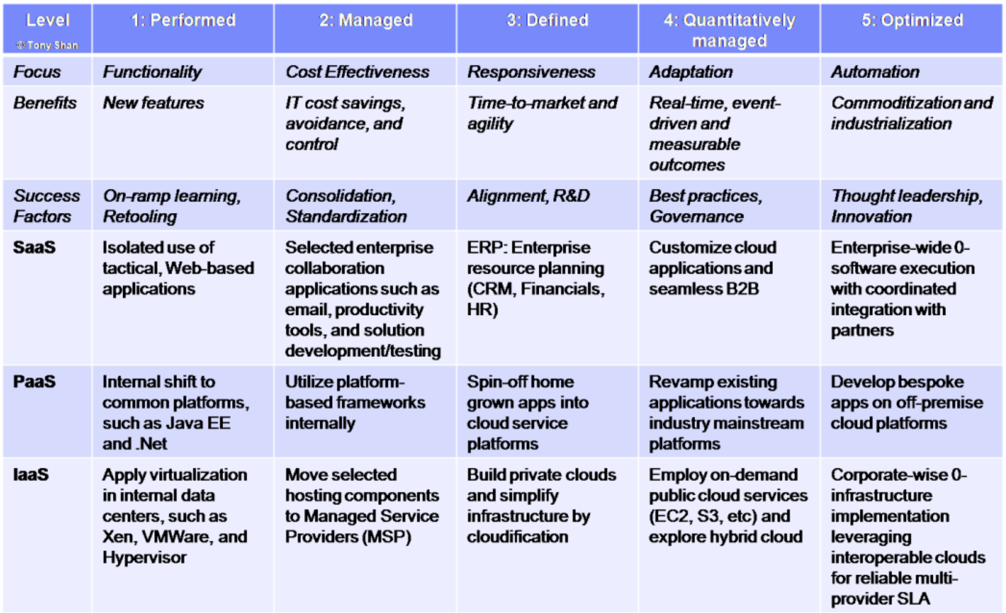
	Return on Investment Calculation of ROI for cloud computing has to consider the time for initial payback. Organization can start from the absolute saving that is realized by all facets of IT operation in relate to workload, including hardware cost, software licenses, upgrade ,system administration, support , end-user support and provision. Some other business-related measures such as increasing user productivity, resource utilization, reduction of risks due to the high availability can be included as well(IBM, 2010b). ROI calculation will shift Capex into Opex for cloud assets since the business model from cloud computing emphasizes on pay-as-you go and organizations won't have to consider upfront investment for public cloud.
Deliverable	**Business Case** A final deliverable from this process is a business case on cloud computing services. Linthicum (2009) defines what should be described in a business case for cloud computing. Since the business case is specifically for adopting public cloud computing to leverage SOA architecture within an organization. Based on his work, we adjust the content of the business case to suiting for different types of cloud computing, the content is described as follows(Linthicum, 2009): 1. A clear understanding of the current business and IT issues the business is facing. 2. The amount of money costs regarding the business. 3. The proposed improvements using cloud computing to address the identified business issues. 4. The amount of money, if any, that can be saved using these improvements. 5. Soft benefits: refer to the value points which are difficult to quantify such as customer satisfaction. 6. Hard benefits: refer to benefits in terms of direct and visible cost reduction and/or business efficiencies that are corrected. 7. Holistic impact on the business: evaluate impact of cloud computing for the business in general such as good or bad; perform risk analysis for the possible occurrences which will influence the business case such as legal changes or market changes; articulate chances that the organization will switch cloud

	providers, and chances that the organization may decide to go from private to public, or vice versa. Planning explicitly about how eh organization will onboard, off board, and switch is critical to the success of cloud adoption(Marks & Lozano, 2010). 8. Final proposed budget.

4.2.2 Create high level adoption approaches

Process Name	**Create high level adoption approaches**
Description	It is useful to set up long term final goals, but short period of delivery strategy is needed. The goal of this process is to ensure that cloud adoption can be under control for a short period of delivery to prevent from failure. In SOA, three types of approaches are usually taken for service delivery, which are(Erl, 2005; IBM, 2010a; Schepers, 2007): • Top-Down: this approach starts from high-level business, structure modeling of services and its corresponding management processes for the service operation, which can be realized for automation later. This approach is time-consuming and requires effective communication within an organization and good translation of business requirements. • Bottom-Up: services are built as needed and they start from problem processes. The approach requires less communication effort but reduces the standardization and reusability of services and it is usually adopted when there are some automated assets. • Meet in the Middle: this approach is the combination of top-down and bottom-up. Top-down analysis is used for the whole project and bottom-up delivery is used for the service. This approach can address the business needs better and require less effort for implementing services. Those three approaches can be taken into account when moving to cloud computing (Rajan, 2010). On the one hand, when applications/services are built from scratch and designed for cloud architecture specifically, the top-down approach will be more appropriate. Organizations can start from a business view that is truly multi-tenant and evolve into a systematic view which supports dynamic infrastructure, elasticity and dynamic scaling.

	On the other hand, when organizations consider moving existing applications to private or public cloud and the applications are not cloud enabled, bottom up approach will be appropriate. Because this approach will enable the organizations to benefit from storage, processor virtualization and on-demand computing gradually. Nevertheless, there are some disadvantages for this approach. For instance, low reusability for the services within the organizations. Meet in the middle approach will share the benefits from both approaches mentioned above. Risks of adopting this approach are smaller because planning and delivery are cutting into small pieces. Nevertheless, aligning top down goals and bottom up experience requires employees to have good communication skills.
Method	Selecting an appropriate approach to adopt cloud computing should work together with a maturity model for cloud computing. The purpose of the maturity model can be used to determine stepwise cloud service delivery within an organization. There are not many maturity models used to evaluate capacity of an organization to adopt cloud computing. The maturity model proposed by Shan (2010) illustrates evolution steps of cloud computing adoption, which can be used as a guideline for cloud adoption within the organization and keep control over the delivery step-by-step. The maturity model indicates that an organization should start cloud adoption from internal to external, from single suppliers to multiple suppliers. In fact, private and public determination can be parallel. The ultimate goal of cloud computing is to achieve commoditization and industrialization of services. As the degree of automation increases, administration cost on IT supportive service will decrease sharply so that organizations can concentrate on their business competitive.



Level © Tony Shan	1: Performed	2: Managed	3: Defined	4: Quantitatively managed	5: Optimized
Focus	*Functionality*	*Cost Effectiveness*	*Responsiveness*	*Adaptation*	*Automation*
Benefits	*New features*	*IT cost savings, avoidance, and control*	*Time-to-market and agility*	*Real-time, event-driven and measurable outcomes*	*Commoditization and industrialization*
Success Factors	*On-ramp learning, Retooling*	*Consolidation, Standardization*	*Alignment, R&D*	*Best practices, Governance*	*Thought leadership, Innovation*
SaaS	Isolated use of tactical, Web-based applications	Selected enterprise collaboration applications such as email, productivity tools, and solution development/testing	ERP: Enterprise resource planning (CRM, Financials, HR)	Customize cloud applications and seamless B2B	Enterprise-wide 0-software execution with coordinated integration with partners
PaaS	Internal shift to common platforms, such as Java EE and .Net	Utilize platform-based frameworks internally	Spin-off home grown apps into cloud service platforms	Revamp existing applications towards industry mainstream platforms	Develop bespoke apps on off-premise cloud platforms
IaaS	Apply virtualization in internal data centers, such as Xen, VMWare, and Hypervisor	Move selected hosting components to Managed Service Providers (MSP)	Build private clouds and simplify infrastructure by cloudification	Employ on-demand public cloud services (EC2, S3, etc) and explore hybrid cloud	Corporate-wise 0-infrastructure implementation leveraging interoperable clouds for reliable multi-provider SLA

Figure 16 Cloud computing Maturity Model (Shan, 2010)

Deliverable

Adoption Plan

Deliverables from this phrase should be an adoption plan. When an organization starts a small cloud computing project, it is likely that the adoption plan will be improved continuously. It is suggested to describe a comprehensive short-term desired outcome first and keep the approach open for long term projects. Normally more than five years ahead of planning will be normal. An adoption plan should include:

- Scope of the projects: for instance, this project focuses on customer data storage service
- Time frame for the project
- Budget
- Responsible parties: sometimes a third party who is responsible for implementation should be clarified.
- Goal of the project: it is better to outline the goals of the project in line with time frame. Long term and short term goals will depend on how the organization will use the method we proposed.

4.2.3 Involving stakeholders

Process Name	**Involving stakeholders**
Description	This process is to ensure that relevant stakeholders get involved when organizations make decisions to go for cloud computing. There are not many differences between introducing a new IT service and a cloud service for this process. Strategic communication will get involved with multiple organizational units, sometimes with business partners to agree on on-going implementation, payment for the service, frequency of business strategy changes and regulation changes. This process is obvious for shared services. For single services, it is still necessary to discuss about the general communication scheme to prevent from silo applications implemented within the whole organization. Even though business strategic change seems to be totally internal decision, yet Cloud Service Providers cannot get out of the process because operation of the services will rely on CSPs' infrastructure(Linthicum, 2009). Successful cloud implementation will have to include CSPs to ensure proper communication, consultation and information when there is a change involved. For example, change management will require collaboration of both internal and external CSP stakeholders to fully understand the consequences of this change no matter the change is from internal cloud consumer organizations regarding strategic or regulation changes or external CSPs' regulation change(Menken & Blokdijki, 2009).
Method	The RACI method can be used to assign what role a stakeholder should take within a project and corresponding responsibilities can be clarified through such type of table. Responsibility (R): people who are expected to actively participate in the activity and contribute to the best of their abilities. Accountability (A): the person who is ultimately responsible for the result Consultation (C): people who have a particular expertise contributing to the decision. Inform (I): people who are affected by the activity/decision but do not have the decision right.

	CIO	Application developer	Enterprise Architect	Process owner	All CoE Member	Service Librarian	CSP
Creating service using PaaS platform	-	R	C	C	I	I	-
Moving data to cloud	A	R	C	R	C	C	C
Change regulation	A	-	I	R	I	I	I

Table 6 Example of RACI table

Deliverable	**Communication Plan** The delivery of the process is a communication plan outlining who should get involved in which stage of cloud adoption initiative and how the communication is performed. The self-service portal from cloud computing enables business departments to bypass the IT departments and make decision on their own(ISACA, 2009). It is dangerous when the existing services have relationship with the cloud services and business department do not hold such a holistic view over the trend of services within the organization, leading to duplicate and inconsistence of services or data. Two steps should be considered for creating a communication plan. First, an RACI table should be created to identify relevant stakeholders and corresponding responsibilities. Second, methods and purposes of the communication should be outlined in order to ensure the agility of service acquisition and modification. In addition, communication medium and frequency should be included in the plan as well.

4.2.4 Determine service model and delivery model

Process Name	**Determine service model and delivery model**
Description	This process is to determine the right service and deployment model for cloud. As stated before, cloud can be divided into three types of service models (i.e. IaaS, PaaS, and SaaS) and four types of deployment models (i.e. private, public, hybrid and

<table>
<tr><td></td><td>community. Small Medium Enterprises will be prone to choose public or hybrid cloud(YGL_Life, 2011) for the sake of their own organizational capacities. While big organizations will be prone to choose private cloud because of the security consideration, particularly when there is specific security requirements from organizations such as banks or governments.</td></tr>
<tr><td><b>Method</b></td><td>Determining service model can rely on the three approaches we have mentioned in 4.2.2. to identify the final service model organizations require. After the service model has been finalized, the organizations can choose their deployment model. This process depends on the capability of the organizations, security requirements and the cost of the services. The business case can be used as an input for defining the scale of risks and cost. In addition, workload can be included as another factor to determine the deploy model. Combination of those factors, a decision table or graph can be created with the scale identified for different types of delivery models. This table can be used a guideline for decision making. Table 7 provides an example of such decision table. Other methods from project management and portfolio management can be reused for the decision making.
<table>
<tr><th></th><th>Risks (data, vendor lock in etc.)</th><th>Cost</th><th>Workload Scalability[2]</th><th>Workload Capability[3]</th></tr>
<tr><td><b>Public</b></td><td>Low</td><td>Low</td><td>Low</td><td>Low</td></tr>
<tr><td><b>Private</b></td><td>High</td><td>High</td><td>High</td><td>High/Low</td></tr>
<tr><td><b>Hybrid</b></td><td>Medium</td><td>Medium</td><td>Medium</td><td>Medium</td></tr>
</table>
Table 7 Example of decision making table for different cloud deployment model</td></tr>
<tr><td><b>Deliverable</b></td><td><b>Cloud Architecture</b>
This process will lead to a new architecture for cloud assets. Within the new architecture, it is better to outline the service categorization in line with the three service models. If other service classification methods have been used, it is better to</td></tr>
</table>

[2] Workload scalability: The differences of workload requirement between peak season and low season

[3] Workload capability: the extent to which organizational IT infrastructure can meet with their expectation

	make clear within one document. Cloud provides the possibility to combine existing non-cloud-based assets with cloud-base assets. Differentiating those cloud-based and non-cloud-based assets (i.e. data, service, process etc.) within an overview architecture document will be helpful for deploying the runtime governance technology, such as policy enforcement (see 4.5). Even within the cloud itself, the scalable capability, the control level will require a more fine-grained documentation. Organizations can create a cloud reference model first and then use the reference model for their own cloud asset mapping. It would be better to connect this cloud reference model to the enterprise architecture in order to understand the position of the cloud assets and the relationship with non-cloud assets.

4.3 Organizational Alignment

This section will concentrate on organizational measurements that support introduction of cloud computing. It outlines what changes in organizational structure are needed and whether new organizational units should be introduced for cloud computing. Organizational alignment will tackle the following questions: How do cloud services relate to organizations? Who is responsible for the cloud services? How are cloud services controlled and how is the knowledge shared? How is the cost allocated within an organization? Processes for this section are identified from the reference model (see Figure 17). Detailed discussion will follow the template described in 4.1.

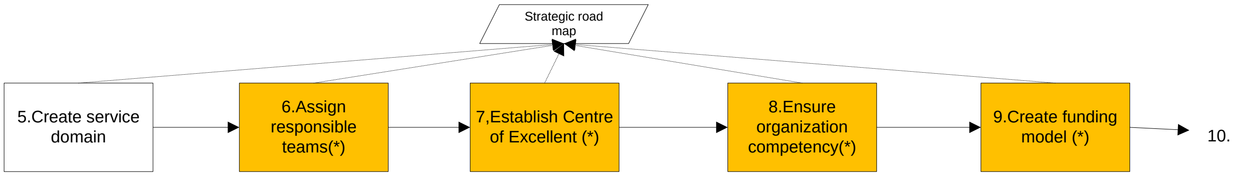

Strategic road map
5.Create service domain
6.Assign responsible teams(*)
7,Establish Centre of Excellent (*)
8.Ensure organization competency(*)
9.Create funding model (*)
10.

Figure 17 Organizational Alignment

4.3.1 Create service domains

Process Name	**Create service domains**
Description	This process identifies and manages cloud service domains and ownership. In SOA, service domains are defined in order to specify the ownership of a service and ensure the success of implementation of the service.(Schepers, 2007; SOA_CoE_Core_Team, 2010; The_Open_Group, 2009). The need to specify the ownership lies in the cross

	organizational boundary characteristic from SOA service. Unclear ownership will lead to problems such as who should pay for the service. As we discuss before, cloud computing service adoption will also have the cross organizational units feature. For private cloud, centralized cloud resource utilization will increase the chance to develop shared service and blur the service ownership. For public cloud, domain and service ownership will be important when services are shared by different departments or organizations. Therefore this process is to make sure that these cloud service can have clear ownership within the organization.
Method	The organization should classify services to understand which domain they belong to and analyze the ownership, which will influence the service funding within the organization. For SOA services, Schepers has identified four types of service domains for, including(Schepers, 2007): • Process domains: service are assigned to end-to-end process, this is applicable to those organizations which works on work-flow and depend on process for their daily activities. • Product domains: services are assigned to different products. This is applicable to those organizations which IT services are served for various products. • Geographical domains: these are suitable for international organizations which coordination is based on different regions. • Functional domains: services are assigned to different functional department. Another ways to define the service domains can base on the services providers' origin(Vordel, 2010), including: • Public domains: Service under this domain is mainly from public service providers such as Google, Amazon etc. • Internal domains: Services are created and can be controlled within the organization. • Partnership domains: Services are from partners; this type of domain is similar as community cloud service described in 2.2. Both domains designation can be applicable to cloud services, and both have pros and

	cons. A better approach for cloud services domain allocation is interweaved those domains together according to their own business needs. For example, several services can belong to one process domain, and those services can be further categorized into public, internal and partnership domains. In such a way, services under the same process domain can have consistent service payment ownership and business policies. On the other hand, the further classification of services will contribute to better policy mapping from different service origins. Internal services and external services will probably have slightly different policies even though they are under the same process domain. Because sometimes some of the performance policies are determined by providers instead of the organization. Another example is that services under one process will have different policies when they belong to different geographical regions.
Deliverable	**List of service domains** The result of service domain will depend on the strategic choice mentioned before. A clear service domain description is important for the following cloud service governance. As noticed before, one cloud service will probably belong to multiple service domains, such as process domain, public domain etc. When organizations have already had mature SOA service domain definitions, it is better to extend those domains to suit for the cloud setting. One the one hand, it will further extend the SOA principles when managing cloud services. On the other hand, cloud service domain can benefit from the existing domain classification.

4.3.2 Assign responsible teams

Process Name	**Assign responsible teams**
Description	When services grow and expand within different parts in one organization, it is emergent to have a team to be in charge of those services and keep an overview on the services. This team can be formed to bridge the differences between management strategy and operation(Schepers, 2007). Collaboration is emergent to require experts within one area to agree on the standard. Experts from different areas are required to agree upon the overall progress. This process is to discuss the responsible team for cloud service management.

Method	Nadhan has introduced two approaches for SOA governance regarding this topic, including centralized and distributed approach[4](Nadhan, 2004). • Centralized approach: in this approach, each service domain is represented into a centralized unit, together with some parties. And the unit is responsible for reviewing added, changed and deleted service before authorizing implementation. • Distributed approach: in this approach, each business unit will be in charge of authorizing changing to its own services. Guidelines will still be defined by a thinned centralized unit, however, standard and ownership will be assigned to each business unit. This approach will probably link to the functional domain as we mentioned in 4.3.1. Private cloud concentrates on resource pooling and scalable provision of internal resources. It emphasizes high resource utilization through virtualization technology in order to support multi-tenant. Distributed approach contradicts to this principle from cloud since this governance team will lead to a separate architecture and diminishing the resource pooling within one organization. Public cloud also emphasizes the swift subscription to services from public CSPs without worrying out up-front investment. When the services are highly separated and communication will not be an issue, both governance approaches can work for public services. Nevertheless, if services are connected to each other, centralized approach will be more appropriate since changing process requires faster decision making process. Besides, as hybrid service grows, centralized approach will facilitate the interoperability and standard selection. Waggener proposed four specific service teams to support the IT delivering, including infrastructure, Application, Data, and Client services(Waggener, 2010). Those teams have to work together to deliver and develop solution for their customers. Even though centralized approach seems more appropriate for the cloud model, team

[4] See appendix D

<table>
<tr><td></td><td>transformation should take slowly. A cloud council can be formed to be in charge of the overall decisions. At least one member from each team should be selected into the council.</td></tr>
<tr><td><b>Deliverable</b></td><td><b>Team description</b>
At the end of this activity, responsible teams should be assigned. Responsibility and the expected roles should be documented. Since transformation should take the organizational culture into count, original organizational structure will probably keep the same at the very beginning while only new roles and new councils will be formed.
<table>
<tr><th>Org. unit</th><th>Responsibilities</th><th>Roles needed</th><th>Relationship</th></tr>
<tr><td>Infrastructure team (existing)</td><td>Ensure infrastructure guideline are followed</td><td>Cloud data architect, Cloud security manager</td><td>Cloud developer team , line of business</td></tr>
<tr><td>Cloud business council (new)</td><td>Ensure cloud fits with business need</td><td>Business Analyst , Cloud service manager</td><td>Line of business management , Developer team</td></tr>
</table>
Table 8 Assigning Cloud Responsibility to organizational units</td></tr>
</table>

4.3.3 Establish centre of excellent

Process Name	**Establish centre of excellent**
Description	Another coordination scheme learnt from SOA is to establish the centre of excellent(CoE) in order to facilitate communication and knowledge sharing(Ovum, 2010). CoE consists of experts from different areas and different parts of an organization. The benefit of CoE is to integrate experience from different departments and ensure faster deliveries of cloud services. When cloud computing begins to spread out in the organization, some regular meetings between the experts will be considered enough as CoE. As cloud computing gets more mature, fulltime professional employees will be needed.
Method	Establishing CoE within an organization can consider the following items: • Document previous experience (e.g. pilot/non-pilot, small/medium project) and communicate to prevent from re-occurring problems.

	• Develop guidelines to accelerate the adoption and incorporate the guidelines into policies. For example, determine the standard of cloud services to facilitate organizational cloud service delivery. • Ensure communication within the organization to advocate the correct use of cloud computing and provide feedback when it is necessary. • Monitor direction: CoE should be responsible for evaluating current performance against the determined strategy as well as ensuring business and cloud service alignment. Operational performance monitoring is not necessarily the responsibility of CoE. CoE as a knowledge centre will facilitate the communication scheme and standardization of cloud computing for the organization. They are not necessarily in charge of creation of governance policies.
Deliverable	**Deliverable: CoE strategic planning** In order to make sure smooth establishment of cloud CoE within organization, CoE strategic CoE planning is required, within which goal and tasks of CoE members should be defined. Proposed CoE strategic planning should include: • Mission Statement : outline the long-term objectives of CoE • Organizational position of CoE: emphasize the authority of CoE within organization and empowerment of this unit. • Responsibility, role definition of CoE. Some actions should be articulated , for instance, training responsibilities • Roadmap of CoE development , which will be linked to the maturity of cloud computing within organizations and the service development or adoption within organizations

4.3.4 Ensure organizational competency

Process Name	**Ensure organizational competency**
Description	Introduction of cloud services will heavily rely on the business requirement analysis and related processes. This transformation will lead to increasing the demand on business and management skill set(CA_Technology, 2011; Waggener, 2010).A majority of roles in

	an organization will be not necessarily changed at the very beginning of cloud adoption. Nevertheless, capability of existing roles will be necessary to be developed in order to cope with new technologies and decision making manners. This process will concentrate on educating existing roles and probably introducing new roles to ensure the right skills and knowledge employees should hold.
Method	Old roles such as system administrator, computer operator, network administrator, storage administrator and database administrator will be still necessary and the importance of those roles will increase because of the cloud requirements. New features of cloud resources and new requirements on vendor management will lead to a demand on new roles such as cloud administrator, cloud architect, cloud service manager and so on(CA_Technology, 2011). Cloud enables business departments to determine the IT resources through a self-service portal, which means that business managers should improve their capabilities to IT knowledge set. The emergent skills include capacity planning, requirement gathering, and project/portfolio management. Service manager and data architect will become more and more important because they play the important roles in coordinating LoB, IT and CSPs. Detailed roles and their descriptions are shown in Appendix E.
Deliverable	**Role Plans** Searching the right people for the new roles or evaluating the competency of old roles to determine the right training plan is challenging in this activity. A better approach for role planning is to first outline all the roles required and competency requirements for those roles. The new role list should try to get close to the existing organizational roles. In such a way, organization can make use of the existing roles and avoid hiring new employees. When such a list has been finished, evaluating the existing roles can start. The evaluation results can compare with the competency requirements we have outlined in previous role requirement list. Training and recruitment plans can be developed on the basis of such an evaluation and comparison results.

4.3.5 Create funding model

Process Name	**Create funding model**
Description	Traditional IT budget can be assigned to business units, project etc., cloud computing can be a centralized IT resource based on usage billing model, blurring traditional

	budget boundary. One of the approaches for an organization is to enable IT department to charge cost back to individual units through implementing a cost model(Cisco, 2010; Creswich, 2010; Settle, 2010). This process concentrates on searching mechanisms to support charge back strategies for cloud computing services within the organization.
Method	The first step is to initiate discussion between cloud owners and prospective users (e.g. different line of business departments) to reconcile different opinions. The second step is to determine the charge back methodology. Three types of charge back approaches have been found in a federal cloud computing environment(Creswich, 2010): • Non-IT-Based Allocation: cloud owners charge back cost to cloud users based on a formula without considering the cloud services they use. The formula could be percentage of the budget. This approach will cause the most dissatisfaction among cloud users. • IT-Based Allocation: 1) Direct Allocation: cloud owners charge back on a fixed basis, using a specific metric as divisor for associated costs regardless of the actual consumption. This approach is useful when actual usage is hard to estimate. 2) Measured Usage: cloud owners charge back cost on the basis of the usage of cloud resources. This approach works well for shared resource capacities (e.g. storage etc.) but some overhead to measure the usage is required. This approach requires the organization to build up automated method to measure the actual usage or public CSPs provide such a usage measure portal for cloud consumers. • Fee-Based Allocation: 1) Tiered Flat Fee: Cloud owners charge back based on the level of effort differences. At the very beginning each cloud user is charged on a flat fee for a basic set of activities. This approach is useful when labor costs associated with the delivery of the services are considered. For example, service desk support. Additional activities will increase the fee on top of the basic fee. 2) Negotiated Flat Fee: cloud owners charge back based on annual analysis of cloud resources. This approach allows cloud owners and users to discuss the

	annual expense from previous years. There are myriad of charge mechanisms from public CSPs, an organization should consider their charging mechanisms to set up appropriate billing approaches within the organization. This approach should be compatible with existing organizational structure and be as simple as possible. Actually for public cloud services, service managers can chargeback LoB based on the invoices and the number of users in each LoB for shared services.
Deliverable	**Cost estimation template** This process concentrates on discovering the charge back mechanisms for cloud computing services within an organization. The challenge is to create visibility for the charge back. It is suggested that cloud owners to create a cost estimation template and use it for communication with cloud users. When public cloud services have been used, it is still important to have such a template because other support activities will probably contribute to the costs of using public cloud services. For example, monitoring public cloud service providers. Some of the items are proposed to consider within the template, including(Creswich, 2010): • Cloud cost drivers: inputs of the cloud cost driver can be derived from the business case; those cost drivers can be elaborated in this phrase. • Chargeback: this item is set to indicate whether those cost drivers are eligible for being charged back to cloud users. • Category: this item is set to indicate the types of cost drivers such as hardware, facilities, software, or labor. • Methodology: this item is set to identify the methodology for charge back. • Rate and unit: this item is set to define the amount of cost that can be charged back for a unit of the cost driver (this cost can base on the benchmark data from the similar services). • Quantity: this item refers to the amount of capacity cloud owner estimated that cloud uses' will consume. • Fiscal Year Costs: this item represents a detailed build-up of expected cost for a service over a period time (e.g. a year, a month etc.).

	One example of the template is shown in Appendix F. Similar methodology can be used by pubic CSP for a visible cost charging from their clients, increasing cost visibility between public CSP and consumer organizations. At the same time, this template will be useful for capacity estimation by CSPs and can be implemented for better resource utilization.

4.4 Lifecycle Management

This section will concentrate on service lifecycle management. Cloud service management starts from creating/requesting a service to termination of a service. Acquisition of a service will depend on the detailed SLA negotiation (see 4.6) and requirements for the service (see 4.4.1). Governance of cloud services will include developing services, delivering services as well as operation time of services. This section is about developing and delivering cloud services. Most of the people refer them to design time services, runtime services is mostly about policy enforcement as well as SLA management, which we will discuss later. Lifecycle management will tackle the following questions: How can an organization ensure the consistency of services when creating cloud services? How can an organization ensure the right behavior of services? How can organization track the status of services? Processes for this section are identified from the reference model (see Figure 18). Detailed discussion will follow the template described in 4.1.

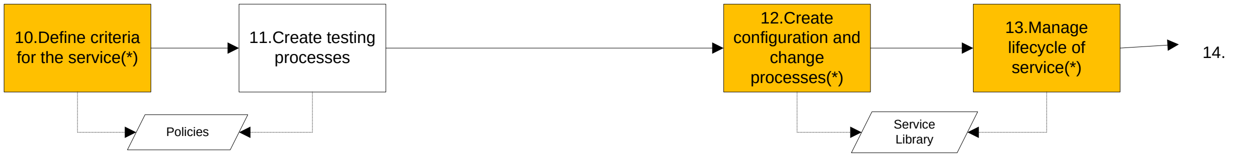

10.Define criteria for the service(*)
11.Create testing processes
12.Create configuration and change processes(*)
13.Manage lifecycle of service(*)
14.
Policies
Service Library

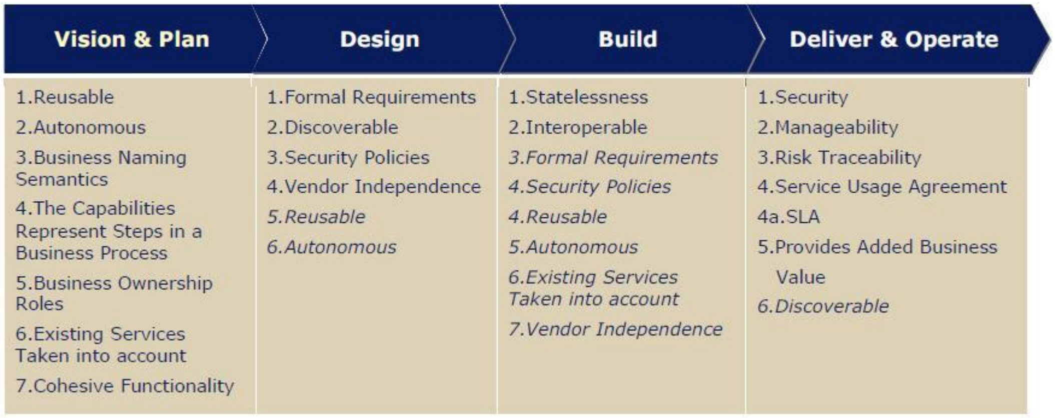
Figure 18 Lifecycle Management

4.4.1 Define criteria for the services

Process Name	Define criteria for the services
Description	This process is set up to define criteria for the services, leading to a set of policies. Technical and organizational demands should be articulated in order to make sure the consistency of those services(Schepers, 2007). Those criteria will be formalized into policies and used to govern the behavior of the users[5] (both developer and end-user of

[5] Those criteria and SLA (4.6) can be considered together when selecting public CSPs.

<table>
<tr><td></td><td>the services such as other business units or the clients of the organization). Since cloud service is based on self-service portal, policies are an important mechanism of imposing requirements on developing and selecting services.

Policies can be business or IT related and creation of the policies should be done earlier in order to make sure successful service deployment. Enforcement of policies belongs to policy management and will be discussed in 4.5.</td></tr>
<tr><td><b>Method</b></td><td>Dow has created a model containing a set of criteria for enterprise services(see Figure 19) (Dow, 2007). Italic criteria are required to revise in that phrase. This model can be used for the basic cloud service creation. Nevertheless some other criteria which are specific to cloud should be added into this model. La and Kim propose to consider three desired properties when an organization designs its SaaS services, including high reusability, high availability, and high scalability(La & Kim, 2009). High reusability has been contained in Dow’s model while the other two do not. High availability emphasizes that the services should be deployed and supported access through Internet. The multi-tenant feature of cloud computing service demands that the services, to some extent, have to support concurrence access by multiple consumers. The other criterion – high scalability- is matched to the feature of cloud computing service too. Since the amount of service requests from end-user such as service load are dynamic and hard to predict, cloud services should be able to support the peak time requests.

<table>
<tr><th>Vision &amp; Plan</th><th>Design</th><th>Build</th><th>Deliver &amp; Operate</th></tr>
<tr><td>1.Reusable
2.Autonomous
3.Business Naming Semantics
4.The Capabilities Represent Steps in a Business Process
5.Business Ownership Roles
6.Existing Services Taken into account
7.Cohesive Functionality</td><td>1.Formal Requirements
2.Discoverable
3.Security Policies
4.Vendor Independence
<i>5.Reusable</i>
<i>6.Autonomous</i></td><td>1.Statelessness
2.Interoperable
<i>3.Formal Requirements</i>
<i>4.Security Policies</i>
<i>4.Reusable</i>
<i>5.Autonomous</i>
<i>6.Existing Services Taken into account</i>
<i>7.Vendor Independence</i></td><td>1.Security
2.Manageability
3.Risk Traceability
4.Service Usage Agreement
4a.SLA
5.Provides Added Business Value
<i>6.Discoverable</i></td></tr>
</table>
Figure 19 Enterprise Service Criteria model(Dow, 2007)</td></tr>
<tr><td><b>Deliverable</b></td><td><b>Policies</b>
Deliverable of this process will be a set of policies supporting lifecycle management.</td></tr>
</table>

	Creating policies should stick to the service criteria definition procedure. When a policy is created, the following items should be articulated: • Formalize policy description with little ambiguous description. • Specify conditions when the services should comply with the policies. • The genus of the service. For example, what type of service you are created? Single tenant or multi-tenant. Policies for multi-tenant services will be different. • Specify audience of the policies. For example, who should know the policies? • Present reasons why the policies are created. It is believed to be helpful that audience or the owner can trace back the reasons for the policies so that they can enforce and update the policies when it is necessary. • Specify exception procedures when a policy can be ignored. • Identify responsible owners for the policies (e.g. IT or LoB departments). • Whether the policies is composed or not. If so, corresponding policies should be articulated. • Specify that the policies are internal or external. Policies can be created by organizations or subscribed from third parties[6]. Identification of the origin of the policies will enable a better policy management. Three types of policies are interested in cloud context(Guo, et al., 2010): • Data policies: data policies include all the relevant metadata within the candidate applications. For example, location of data, data structure, logical and physical model, security issues on data, and so on. • Service polices: service policies include all the relevant meta-service information. For example, whether the service is loosely coupled? Where the service is resided, on premise or cloud? Is the service composite or not? Who can manage and govern the services? • Business process management policies: the policies include the way how web services and cloud-based services work together. For example, business logic, sequencing, exception handling, process decomposition as well as process reuse.

[6] The cloud computing model enable that some types of polices can be subscribed through internet, for instance, security policy with regard to a service can be obtained through Internet. Discussion on whether this type of policy enforcement will be put into section 5.

4.4.2 Create testing and validation processes

Process Name	**Create testing and validation processes**
Description	Besides defining relevant criteria for the services, another way to ensure the right behavior of services is through testing. A good governance model should at least include testing processes and relevant tools for the testing. Centre of Excellent can coordinate with other business units to specify testing tools and processes. Contracts are usually used as the guideline for testing(Menken & Blokdijki, 2009). Challenges of testing cloud services include: • Developers and testers of cloud-based applications who use remote services generally do not have controllability or observability of the services except the exposed interface(King & Ganti, 2010). • Testing services on top of cloud infrastructure has some limitations. For instance, determine saturation point to find out upward limitation on scaling or crash down the system would not be wise to put into cloud service testing(Linthicum, 2009) • Validating applications which use stateful cloud services will be difficult, this traces back to the service criteria creation (see. 4.4.1.2), and service developers should try to make a statelessness service. • The usage pattern for cloud services such as how one system interacts with another will be different from the one for on-premises services; internet connectivity has to be considered (Linthicum, 2009; Riungu, Taipale, & Smolander, 2010). Cloud Services can briefly be categorized into on-premise and remote services. We concentrate on the remote cloud services because most of the challenges mentioned above are related to remote services. Let's recall the testing approaches in software development: white box and black box. Black box testing is more applicable to cloud testing concept since consumer usually don't own the cloud system and control over the cloud system, at least most of the providers have not support them yet.
Method	A regression testing V model proposed by OCG can be considered as a baseline for cloud testing (See Figure 20).The level of test is derived from the way a system is

designed and built up. Instead of moving down in a linear way, the process steps are bent upwards after the coding phase, to form the V shape. The left-hand side stands for the specification of service requirements down to detailed service design while the right-hand side represents validation activities against the requirements on left-hand side. Advantages of the V-model are that by executing tests at the time of specification formulation, errors in the specifications can be detected in an earlier phase, avoiding costly reworks later on(OCG, 2011). Relate to this Service_V_Model, it is suggested that testing level has to reach 4 or 5 level in cloud setting(Menken & Blokdijki, 2009).

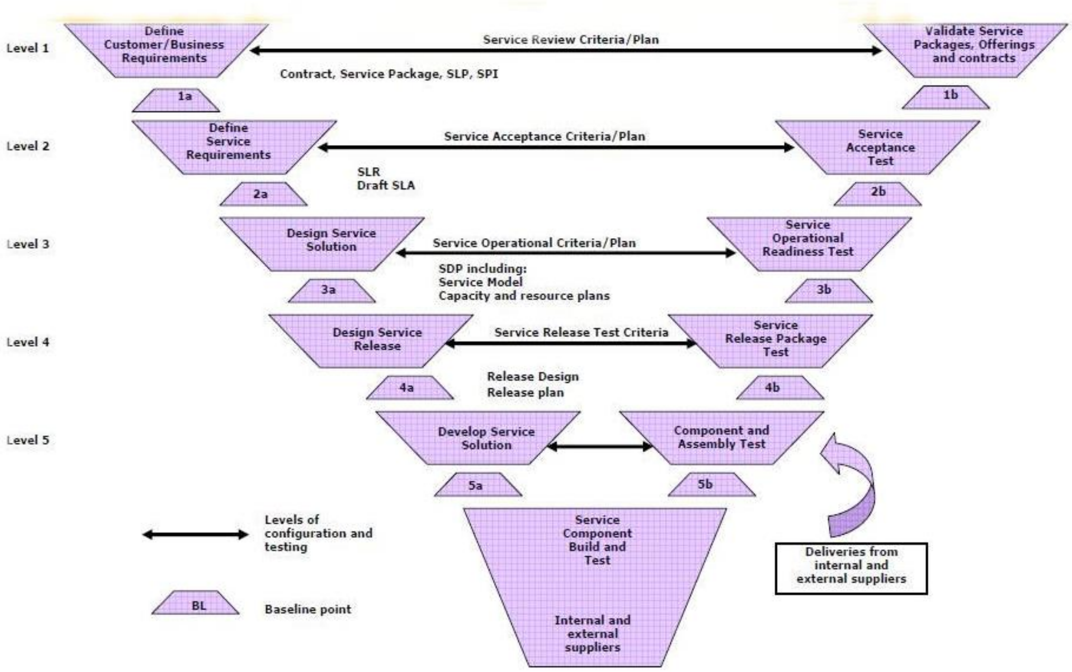

Level 1
Define Customer/Business Requirements
Service Review Criteria/Plan
Validate Service Packages, Offerings and contracts
Contract, Service Package, SLP, SPI
1a
1b
Level 2
Define Service Requirements
Service Acceptance Criteria/Plan
Service Acceptance Test
SLR
Draft SLA
2a
2b
Level 3
Design Service Solution
Service Operational Criteria/Plan
Service Operational Readiness Test
SDP including:
Service Model
Capacity and resource plans
3a
3b
Level 4
Design Service Release
Service Release Test Criteria
Service Release Package Test
Release Design
Release plan
4a
4b
Level 5
Develop Service Solution
Component and Assembly Test
5a
5b
Levels of configuration and testing
Service Component Build and Test
Deliveries from internal and external suppliers
BL
Baseline point
Internal and external suppliers

Figure 20 The Service V-Model(OCG, 2011)

Linthicum further breaks down cloud service testing into the following aspects(Linthicum, 2009):

- Service level testing: create a list of use cases and store them for reuse(Benedetto, 2006); list candidates which use the same service or components and test them together; test heterogeneity of the services to ensure platform independence; differentiate on-premise and remote services; create instance and test the result to tackle the abstraction from cloud; use holistic testing for aggregation services.
- Security-level testing: the best approach is to start from understanding the

	security requirements for the services and create a testing plan by concentrating on the vulnerabilities such as information security issue and denial-of-service attack, malicious service and so on. Black-box testing is found to be appropriate for this type of testing. • Process Testing: since processes are sitting above services, bottom-up approach is preferable. • Policy testing: because some of the policies will be enforced during run-time (see 4.4) to ensure the right usage behavior regarding those services, testing the policies and ensure that they can behavior as expected is important . • Integration Testing: this is similar as traditional service testing; the purpose of integration testing is to ensure that all the interfaces (e.g. behavior and information sharing between services) work correctly. For instance, whether the communication can be established with late binding or whether the transmitted information is accurate in semantic. • Information Testing: it is mainly about testing the data persistence layer, typically the database, without going through the services. It will ensure the behavior of the database from performance, stability, interface efficiency and schema efficiency. • Performance Testing: the testing is accomplished through creating a performance model to address how the cloud system will perform under different workloads. It will help to determine where the bottleneck is (e.g. database, network or the service).
Deliverable	**Testing Plan** The content of testing plan will be various for different testing cases. For cloud services, testing plan should concentrate on security requirements and SLA compliance. Integration testing should be paid attention to when the services are from multiple cloud vendors or the services are mixed with on-premise and cloud components. Loosely couple principle should be considered when developers design such type of services in cloud.

4.4.3 Create configuration and change processes

Process Name	**Create configuration and change processes**

Description	This process is about creating configuration and change processes. The main concern for configuration management is to manage the information related to cloud services/resources. The main concern for change management is to take care of various end-user requests to change the services. For example, requests to extend, modify, terminate of existing instances. These two processes, to some extent, have related to each other. For example, when a user request a new VM, cloud management system will initiate a new instance of VM, leading to new information regarding the VM stored in the configuration database. Change and configuration management play an important role in cloud as other IT services. Consequence of inappropriate change and configuration management will lead to breaking down the whole running system and result into a huge lost for the business(Guo, et al., 2010; Linthicum, 2009; Microsoft, 2010). The two management processes are harder in cloud because cloud resources include various resources (e.g. hardware and software, physical and virtual, private and public resources), resulting into a more complicated dependency issue (The_Open_Group, 2009). On the other hand, cloud computing emphasizes flexibility and agility, which means the frequency to change the configuration baseline will be higher and it demands less time for the change. What's more, the invisibility to the underlying infrastructure from public CSPs will probably increase the difficulty for these two processes(Hurley, 2010).
Method	**Configuration Management** In fact, it is not necessary to have complete transparency to obtain an appropriate level control for configuration management. Consumer organizations can do nothing to solve the issues if they find out that there are some problems related to the infrastructure from public CSPs. Therefore they should focus on the things they can control and manage the rest via contractual negotiations around SLAs with their CSPs(Hurley, 2010). As the types of cloud influence the control level from consumer organizations, the Configuration Items (CIs) which the organizations should store for management will be different.

For public cloud, the main CIs should include the information that represents the service type, providers' name and their SLAs. For private cloud, the information should include the SLAs offered to the business users of the service, the service type, and a set of infrastructure elements which support the cloud services.

For SaaS, consumer organizations will have various visibilities into the applications but have no visibility into the infrastructure. The main information should include attributes used to initiate the applications such as owners, requestors, duration, purchased availability, and bandwidth.

For PaaS, the main CIs should include the instantiation information pertaining to the hosted applications. In addition, information from SaaS should be included as well.

For IaaS, the main CIs should include initiation attributes which support the hosted virtualized systems. The systems will leverage other upstream CIs to provider services. The upstream connection can be the public or private clouds on which the IaaS resides.

Change Management

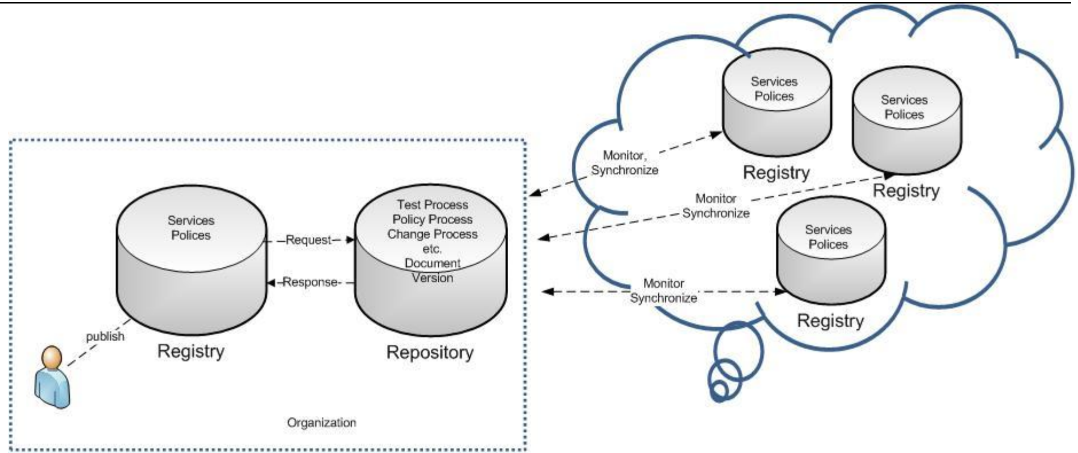
In order to have a precise procedure for changing the services in cloud, the following issues have to consider based on the traditional change process(Colville & Spafford, 2010; Hurley, 2010; Menken & Blokdijki, 2009; Schepers, 2007):

- Ensure that there is a suitable business case for the change to progress through each of its major stages. Business case should contain the impact of change in relation to laws, regulations and other risk factors.
- Identify whether there are adequate resources (financial, personnel and other) for the change.
- Ensure that interfaces and dependencies existing in those cloud environments are considered during the requirement elicitation phrase to avoid conflicts.
- Establish a thin authorization process and standardize the change processes: In order to support the flexible change requirement for cloud, it is better to standardize the changes that occur with enough frequency, classify them and

	record relevant conditions that triggers the changes (e.g. an authorized request for the service, a trigger load event). The conditions should be reviewed and approved by the authority before. • Automate updating the baselines stored in CMDB: since the change will influence the versions of CIs stored in CMDB, it is better to automate the update to save the administration effort. CMDB can keep track of different version of CIs and change record so that the information can be used for problem management. • Changes made by CSP should be identified and managed appropriately: When the changes are initiated by CSPs, CSPs should notify the responsible contactors in the organization about the changes through dashboard or other notification channels so that they can evaluate whether those changes will influence the services running upon the cloud. • Track software licenses: Consumer organizations should create the ability to document and discover license installation in order to cope with the dynamic challenge cloud computing brings to tracking the usage of software and applications.
Deliverable	**Configuration database and change processes** Deliverables for this process will be a configuration database which records the relevant information for change and problem management and a set of standardized change processes. Consumer organizations should focus on the things they can control and leave the rest to their providers through contract negotiation. Normally, some configuration databases(CMDB) offers mechanism and specifications for federation(Plummer, 2010), enabling the CMDB from consumer organizations to synchronize the information with their CSPs. The change process and configuration management procedures from ITIL framework can be still applied to cloud services(Mather, Kumaraswamy, & Latif, 2009), however, there is a need to modify the process into a thin authorization process so as to cater for the flexible change requirements.

4.4.4 Manage lifecycle of services

Process Name	**Manage lifecycle of services**
Description	Previous activities have contributed to a list of processes and policies regarding the control over cloud services. This process is to consider implementing supports for those processes. In SOA, authorization and lifecycle management is supported by registry/repository tools (Keen, et al., 2007; Schepers, 2007; webMethods, 2006). Authorization is set to ensure the right for publishing, selecting, and changing the services or its associated policies. SOA governance relies on those registry/repository tools to store and manage services and its meta-data. The tools can also be used to store processes and support policy enforcement, ensuring the runtime service behavior. Policy enforcement will be discussed in 4.5. As cloud services expand and grow in the organization, the increasing number of services will enlarge the difficulties to manage and control the services. Service registry/repository from SOA can be leveraged to cloud service for tracking status of cloud services (Guo, et al., 2010; Linthicum, 2009; O'Gara, White, Rajan, Roman, & MacVittie, 2009). Service registry/repository for cloud should support federation with its own integration environment, multi-enterprise collaborative environments, cloud environments, system management environment and business process management environment(Plummer, 2010).In addition, the registry/repository should be able to capture virtual artifacts and support managing different tenants. Federation capability can be realized through a master registry or delegated system(Plummer, 2010). In a master registry system, every registry synchronizes or communicates with a parent registry that is the “system of record”. In delegated system, every registry synchronizes or communicates with its sister registry and hands over information. Figure 21 illustrates a master registry/repository system. The registry and repository at left-hand side is the master registry/repository.

	 Services Polices Registry publish Request Response Test Process Policy Process Change Process etc. Document Version Repository Organization Monitor, Synchronize Monitor Synchronize Monitor Synchronize Services Polices Registry Services Polices Registry Services Polices Registry Figure 21 Registry/Repository for cloud services
Method	The cloud registry/repository should have the functions such as publishing services, taxonomy of service and assignment ownership to services as SOA registry/repository. Other key functions that the registry/repository should have, are outlined as follows: • Authorization for the services: this function will ensure proper authorization of selecting, accessing and changing service. It will be vital as more and more cloud services are adopted within the organization(s). • Dependency of services: both vertical dependency and horizontal dependency should be considered. Vertical dependency refers to the dependency among cloud stacks such as SaaS services and its dependent virtual servers or platforms. Horizontal dependency refers to the relationships among different components running at different cloud platforms. The dependency information can be used for the impact analysis in the change process. • Store policy references and its version: Policy enforcement will be discussed in 4.5. • Store policies and its associated service. • Support impact analysis: This function correlates to the change process. When a service is changed, change process should be triggered. • Support synchronization with other systems: when only private cloud services are adopted, the synchronization function will enable the private cloud services to be consistent with the existing services. When public cloud services are adopted, the function will enable policies for the private cloud service to be

	reused into equivalent public cloud services. In addition, it allows both consumer organizations and CSPs share the updated information(Open_Cloud_Standards_Incubator, 2010). • Support virtual infrastructure provision or both virtual and physical infrastructure provision: detailed functions depend on the scope of requirements and use cases. For instance, whether the registry/repository should support public or private cloud provision or both(Scott & Colville, 2011). The registry/repository should support rule-based automated resource provision. • Image library: the registry/repository should contain frameworks for maintaining multiple repositories of sever images(IBM, 2011b). • Support metering cost and usage for shared private cloud service (see 4.6)
Deliverable	**Automating service lifecycle support** Service lifecycle support for cloud computing includes configuration management (see 4.4.3), authorization management, real-time resource provision, policy enforcement, SLA management and so on. Functions of such a product will be various because the targets of vendors and their strength are different. Evaluation on all the available products and different requirements for various consumer organizations will be impossible for the thesis because of the limited time frame. For consumer organizations, they can start from analyzing their current and future requirements. A comprehensive tool is not necessary for all the organizations. Simple tools can be considered to cater for the current needs. Other tools can be added as the needs grow in the organizations.

4.5 Policy Management

Policy management will invoke after cloud services are deployed. Policies are business rules, which are created by previous activities. Problems such as ensuring quality of services, authorization and security can be solved by policy management. Policy management will tackle the following questions: How can organizations put policies into place? Where the policies should be enforced? How can organizations deploy and track the policies? (See Figure 22).Detailed discussion will follow the template described in 4.1.

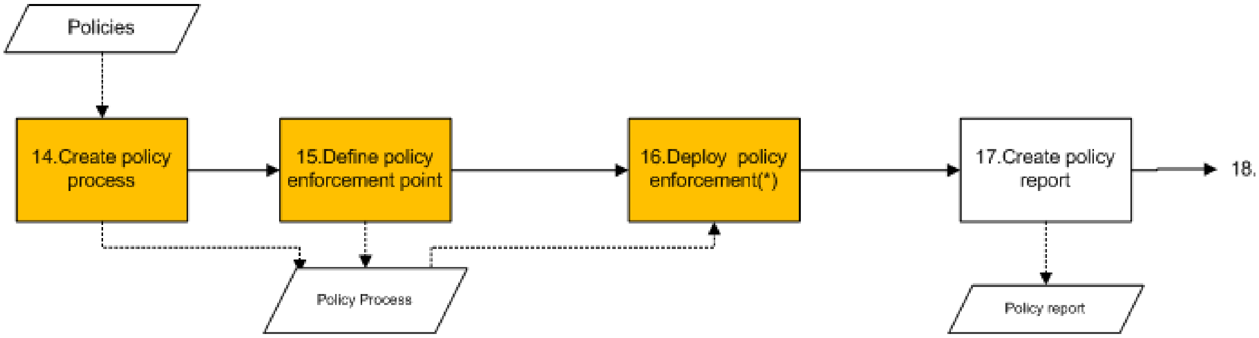


Figure 22 Policy Management

4.5.1 Create policy processes

Process Name	**Create policy processes**
Description	Policy is one of the main components for governing cloud computing services. Creating policies and enforcing the policies will become one of the activities within the organization. Challenges of managing the policies will increase when more participants from different best practices need to contribute to increasing the relevance of those policies(Guo, et al., 2010). Policy processes are created to confront with those challenges through an agreed workflow around policies, policy enforcement, authorization and people who should perform those activities. Policy lifecycle management from SOA includes(Hondo, Portier, & Potepan, 2008; Schepers, 2007): • Create policy: policies are created through a person who is familiar with cloud service criteria or requirements. S/He is responsible to transform the service criteria into understandable policies. Policies can be first created in papers or other human readable documents. Later they will be translated to electronic policy expression supporting automatically enforcement. • Agree on policy: policies should be verified after creation and ensured that there is enough support to enforce those policies. This can be done through establishing a committee rather than relying on one person for the policies. • Enforce policy: policy enforcement includes design-time and run-time enforcement. Run-time enforcement is more important for cloud context and we will explain in 4.5.2 and 4.5.3. • Monitor and evaluate policy: policy should be reevaluated after a period time on the basis of the collected statistics. Corresponding reports should be

	created. For instance, when a security is obsolete, it is necessary to make some changes. Details on monitoring and evaluation on policies will be explained in 4.5.4. We identify there is another emergent activity for cloud computing, which is mapping policy and it should be placed before policy agreement. Mapping policy focuses on identifying policies for private cloud and reusing them into public cloud services, resulting in a consistent way to manage cloud services as a whole. If several public cloud services are identified as candidate services, it is also necessary to compare and match the policies from those candidate services for a consistent policy management. In fact, managing policy manually will be an intensive job and it will be better that the registry/repository can support policy federation with their suppliers. Communication on the policies can be implemented through dashboard or email notification to relevant roles, department and business functions(Guo, et al., 2010).
Method	Consumer organizations should strike a balance between flexibility and control when creating policies and policy processes. The ultimate goal for policy management is to establish a more agile-based decision making capability within the organizations without losing rigidity and security. When creating a policy process, organizations should consider the following issues: • Assigning ownership to both policies and policy processes • Handing complaints should be included into the process • Add mechanisms for policy mapping, the mechanisms should support policy reuse and require less administration effort. If managing external public policy takes too much effort, automating policy synchronization should be included into relevant tools. For example, the tools should support policy federation. • Review policy should align with the organizational goals. Output of the review can be used for updating policy mapping mechanisms. Reports from internal and external cloud should be combined as much as possible, resulting into a concise and consistent notification and alert.
Deliverable	**Policy Processes**

	Deliverables of this process are the policies processes which are used to ensure policy management. Some of the items should be considered: • Define a workflow used to specify those five activities for policy management • Identify a bundle of decision points to determine who need to authorize a policy and what should be done for approval and disapproval. • Describe policy into a template, leading to a pre-built template.

4.5.2 Define policy enforcement points

Process Name	**Define policy enforcement points**
Description	This process aims to define policy enforcement points for cloud services. Policy enforcement is about implementing policy process against situations to check policies. As stated before, policy enforcement point can vary from human to automated enforcement points, from design time enforcement points to run-time enforcement points. Design time policy enforcement is usually related to service development process or service acquisition process. Run-time policy enforcement is about enforcing policy when a service is executing. Run-time enforcement is more interesting to us because the automated enforcing policies can suit for agile and scalable cloud service and support self-service proposition of cloud computing, ensuring service behavior during execution (Lang, 2010a). In SOA, policy enforcement is implemented through message transport layer. This layer can be in the form of Enterprise Service Bus (ESB) or Communication broker. These message transports can support some runtime policies for SOA services. By considering the requirements from SOA (webMethods, 2006), we generalize the basic requirements for message transport layer to support runtime policy enforcement for cloud services, including: • Consumer identification and security: Identify consumer applications and ensure only authorized accesses for the services. Enable to configure security at runtime. For instance, encryption, digital signature and logging for tracing and tracking. • Routing rules: configure run-time routing rules so as to address performance,

	version management and so on. For example, version-based routing can be used to support version management. • Service Level Agreement management: policies are performed to manage performance and availability to match requirements of an SLA. In cloud, service level agreement management is part of the responsibilities from cloud service providers. The policies will be defined and applied by service providers to ensure the availability of the services they provide. Nevertheless, for cloud service consumers, it is better to define their own polices to prevent the situation when SLAs cannot be met by CSPs. For instance, when the services from CSP fails and a request can be routed to a backup service from other providers or internal comparable services. • Logging, monitoring and alerting: this function is related to the previous function and concentrates on tracking failure or violation regarding the predefined SLAs. In short, policy is not just a way of articulating and enforcing security requirements, it is the integration glue between systems to enable business and IT alignment through offering high level contract like SLA and billing as well as low-level details such as dynamic routing, failover, and data transformation.
Method	Policy Decision point (PDP) is the place where decisions should take place within a workflow. It stores decisions related to security requirements, Quality of Service and decisions when capturing an event from public cloud. Due to the mobile and dynamic nature of cloud service, policy enforcement point (PEP) is used to determine where policy should be executed. PEP enables to decentralize the PDP through language such as Extensible Access Control Markup Language (XACML) so as to associate subjects and objects security targets along with rules for authorization condition and action. Therefore, execution of policy could be mapping namespace, resources, identifiers, channel and objects(Peterson, 2010). PEP usually is placed close to services, some of enforcement points have been identified in cloud context (Layer7, 2011),including: • Policy enforcement on outgoing traffic through placing PEP on the organizational demilitarized zone (DMZ) or Enterprise Service Bus, which will allow the organization to discover who is attempting to use cloud services and

manage it. For instance, when an employee using credit card to access a new SaaS service, stop an unsanctioned used of PaaS components and regulate the use of IaaS.

- Policy enforcement on incoming traffic[7]: it will enable managing the traffic entering. In such a way, it will enable only authorized cloud service can access the IT resource within the organization.
- Policy enforcement on cloud services: deploy virtualized, distributed virtual PEPs in front of cloud applications. Virtual PEPs can optionally deploy throughout the organization. As applications/services move to cloud, those service will bind to the virtual PEPs which are also resides in the cloud. The virtual PEP allows application owners to protect and manage their services. Application-level policy enforcement will ensure fine-grained access control and in-depth understanding of use patterns of actual services, protect data and applications, and manage distribution requests to virtualized application instances. If components are located in both on-premise and cloud, PEPs will enable to govern hybrid applications.

Private cloud, ranging from IaaS to SaaS, can benefit from current on-premise SOA PEP solutions. Opportunities to deploy SOA PEPs into public cloud depend on the control boundary between cloud consumers and CSPs. Cloud-based PEPs are virtual appliance that consists of a policy execution engine operating under a security-hardened and performance optimized operating system. Deployment of virtual PEPs in the cloud needs a customer-accessible hypervisor[8] execution environment(Morrison, 2010).

SaaS applications offer no real chance for SOA PEP deployment because they are implemented as thin client web-applications and only minor configuration is open to consumers such as saleforce.com or Gmail. Policy enforcement for web applications, which simply includes basic authentification, SSL/TLS transport protection, is generally integral to the host application servers owned by CSPs.

[7] Incoming traffic monitoring is also accomplished through implementing PEP on DMZ or ESB.

[8] A hypervisor, also known as a virtual machine monitor, is platform that facilitates configuring and managing multiple virtual machines

<table>
<tr><td></td><td>In PaaS, policy enforcement can be naturally connected to PaaS platform to allow automatically technical policy generation and service monitoring during run-time. How can policy enforcement points are built into PaaS platform depends on(Lang, 2010b):
<ul>
<li>Whether public PaaS platform allows installing policy-enforcement points.</li>
<li>Whether public PaaS platform supports the standards such as OASIS XACML.</li>
<li>Whether public PaaS platform support proprietary policy enforcement points.</li>
</ul>
<p>Thus, the opportunity for deploying virtual PEP appliance in PaaS is also limited. Even though PaaS offers control to customer access to an application deployment environment, the container execution model is still too restricted to support diverse connectivity and operate requirements of a mature SOA PEP code base(Morrison, 2010).</p>
<p>In contrast to SaaS and PaaS, IaaS has the most freedom. CSPs such as Amazon shift the boundary of consumer control to an abstracted hypervisor, enabling to host a virtualized PEP and virtualized subordinate SOA service under PEP management. PEP allows consumer to reassert controls over IaaS-resident applications and offset the loss of low level, physical control by CSPs.</p>
<p>There are two popular ways to enforce policies, including the use of agent technology and network of proxies. Agent technology provides the possibility to proactively monitor the services. However, it is believed to be impractical to reengineer the existing services. Therefore, a proxy or gateway approach is more common for appliance vendors.</p></td></tr>
<tr><td><b>Deliverable</b></td><td><b>Determine enforcement mechanisms</b>
In the method section, we have discussed SOA policy enforcement points and the possibilities of different cloud service models support the extension of SOA PEP enforcement. In general, what CSPs can offer limits the enforcement mechanisms. It is suggested to follow the principle that integrating cloud enforcement mechanisms with SOA enforcement mechanisms as much as possible in order to increase the consistency.</td></tr>
</table>

	Before final decisions are made, it is necessary to check the following items: • The location of the services, internal or external, so as to determine and explore enforcement possibilities from existing governance mechanisms such as SOA. • Evaluate the control boundary exposed to cloud consumers from CSPs. • When possible, discover alternative control mechanisms to complement with the inefficiency of control level from consumers' side. For example, put some requirements on SLA. • Will the decision points be easy to scale and meet the future change?

4.5.3 Deploy policy enforcement

Process Name	**Deploy policy enforcement**
Description	Previous activities introduce a set of policy processes and discuss the policy enforcement points. This process concentrates on finding solutions to support automatic policy management as a whole. In section 4.4.4, we have introduced the service registry/repository to support lifecycle management of services. This registry/repository will also support policy enforcement and management. Policy enforcement requires message transport (e.g. ESB) to connect with registry/repository to find the correct services and enforce policies associate to the service so as to ensure the behavior of the services at run-time (Almaden_System, 2010). Runtime-policy repository will load the policy rules (generated by the repository) at deployment time and distribute them to policy decision points on the protected application platform. When all the messages are passing the policy enforcement points, statistics can be collected on the PEPs and used for incident and auditing analysis. The incident and auditing result can be used for policy update. We summarize the idea about the policy enforcement in Figure 23.

<table>
<tr>
<td></td>
<td>

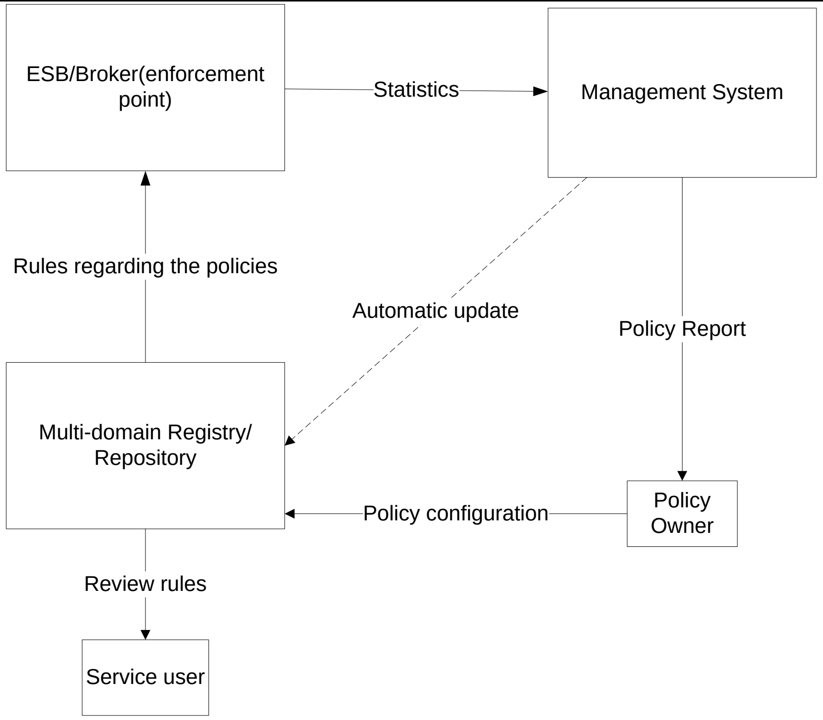


Figure 23 Policy Enforcement mechanism(Lang, 2010a; Schepers, 2007)

</td>
</tr>
<tr>
<td>

Method

</td>
<td>

The Repository/registry plays an important role in supporting policies enforcement. Here we will discuss the requirements of the registry/repository for policy management. The results are shown as follows:

- The repository should store references of the policies.
- Support assigning responsible ownership for the services and policies: When there are some requirements for maintenance such as bug, the responsible person has to take care of the issue.
- Enable multiple versions of policies and services: When a service is changed , it triggers a process to find a new and right policy for this service (Schepers, 2007)
- Support automatic run-time update of policies (Lang, 2010b): Anytime when a policy is changed, policy enforcement and transformation should be executed automatically in order to reduce errors introduced by manually policy management. Automated policy updating ensures that the new policy will replace the old one, associate with right services and behave correctly as expected. Automatic policy update will become promising for policy management as more and more cloud services are adopted within the

</td>
</tr>
</table>

	organization(Lang, 2010a). • Connect policies with impact analysis: when a policy is altered, the change process connected with the services which use the policy should be triggered. • Support audit trail and logging(Guo, et al., 2010): the registry/repository should support tracking the execution of services and policies. For example, what they do, when they are performed and who works on them. The information can be used to determine why problems happen and identify approaches to prevent them. In addition, audit is one of the requirements from many legal compliance standards. Audit information should be also cryptographically secured to prevent disclosure of sensitive information, leading to expensive computation during runtime and low performance. • Ensure that services can be only accessed by the authorized ownership. Credential services with sensitive data and infrastructure should be kept away from intrusion. • Inform consumers when there is a change. • Support multi-tenant security specification of items. For instance, resource data isolation, network isolation with security of virtualized network (Open_Cloud_Standards_Incubator, 2010). • Should leverage long-term, scalable storage in cloud environment in order to mitigate potential loss of data on instance termination.
Deliverable	**Centralized policy and configuration repository and registry** Cloud-centric registry/repository is required as an important infrastructure component for cloud-based PEP enforcement. Currently some vendors have extended their SOA governance products into cloud, including Vordel(Vordel, 2010), Layer7 (Layer7, 2011). Evaluating the capability of those products is out of the scope of this thesis. The cornerstone of cloud governance is policy monitoring and enforcement. Integration with the registry/repository for consistent lifecycle management, policy and service description can be realized later when the usage expands.

4.5.4 Create policy reports

Process Name	**Create policy reports**
Description	Policy reports include the summary of active policies and relevant enforcement. It will indicate a list of services influenced by one policy. Policy report can be treated as an important mechanism for organizations to check against policy enforcement. Automatic policy report generation is preferable(Lang, 2010a). Policy enforcement point typically generates security-related runtime alerts. For instance, one event for the invocation has been blocked. We can call them policy exceptions. The alert information can be carefully monitored ,recorded into the report, and delivered to relevant stakeholders through email(Guo, et al., 2010). Report can be also sent on regular basis, such as at the end of one month. If the reports cannot be generated automatically, it is suggested to use manual reports within the organization(s). Benefits of the manual reports will be the same as the automated reports. Reports can be collected by one responsible owner. The person will have to interview the relevant stakeholders, including public CSPs. Modification on the policies will probably happen as a result of the interviews. Schepers suggests creating one report for a series of policies in relation to one stakeholder because it will save time for stakeholder analysis(Schepers, 2007).
Method	Policy reports can be generated by the registry and repository. Because it keeps tracking the runtime binding of services and the execution of policies. Number of exceptions and compliance to the policies should be summarized here. It will be better that the reports can be customized by consumers. If enforcing policies can be only conducted from service providers, consumer organizations should request CSPs to deliver such reports when they negotiate their contracts.
Deliverable	**Report Template** At the end of this step, a desired report should be created so that monitoring can be applied as services are deployed. Within a report , the following item should include: • What is the report about? For example, a ratio of exception per request. The

	subject of the report should be clear and there should be no discussion on the interpretation. • Why is the report created? • When is the report generated? Is it a periodical report or on-demand report? • Where is the report built? Is it the report created by CSPs or consumer organizations? If the report is created by CSP based on their own information, consumer organizations should consider auditing the report. Sometimes automated and manual report should be made clear as well. • Who is responsible for this report? It is better for the person who is interested in the report to design the report or understand the report provided by CSPs.

4.6 SLA Management

While policy management concentrates on the internal policy management, ensuring the quality from CSP[9] greatly depends on good service level management. This process is responsible for setting qualitative targets and evaluating the service in line with the targets. Cloud consumer organizations can rely on SLA management to decide what they want to do with cloud services. For instance, should organizations add in more virtual machines? At what price point will the option become too expensive to justify the return? SLA management will tackle the following questions: What can be expected from a service? Who is using my service? Do the services deliver the value as I expect? (See Figure 24). Detailed discussion will follow the template described in 4.1.

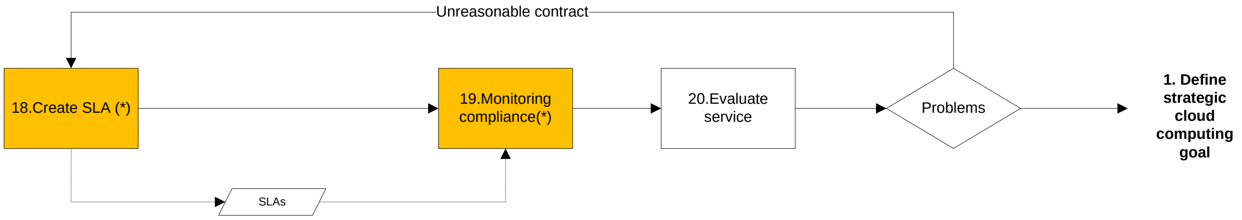


Figure 24 Service Level Management

4.6.1 Create SLAs

Process Name	**Create SLAs**

[9] Both public CSP or private CSP

Description	Service Level Agreement is a contract between cloud service consumers and cloud service providers. There are two types of SLA in cloud, including off-the-shelf SLA and customized agreement. Most of CSPs offer off-the-shelf non-negotiable SLA(Cloud_Computing_Use_Case_Discussion_Group, 2010). For the companies who have more requirements on the data and applications/services implemented in cloud, the non-negotiable SLAs are probably not acceptable. Therefore, consumer organizations should evaluate the SLAs and the business requirements before moving to cloud, especially to public cloud. In SLA, Service Level Objectives (SLOs) are the targets used to determine measurable conditions such as parameters of throughput, data stream frequency, availability percentage and so on. Sometimes urgency rating should also be clarified within SLOs to determine the priority of different parameters. For instance, availability is important than response time. An acceptable SLAs should contain(Cloud_Computing_Use_Case_Discussion_Group, 2010): • A list of services which CSPs will deliver and a complete definition of each service. • Metrics to determine whether providers are delivering services as promised and an auditing mechanism to monitor the services. • Responsibilities of providers and consumers • Remedies available to both providers and consumers if terms of SLA are not met. • A description on how the SLAs will change over time. The purpose of SLAs is to help cloud consumer organizations to make decisions on the way how they use cloud services. As SLA negotiation will probably take too much time and damage the flexibility brought by cloud computing, it is better to automate SLAs as much as possible.
Method	By using Web Service Level Agreement (WSLA) or SLAng to interpret SLAs, the efficiency of service contracting is highly enhanced because the automated negotiation function helps reduce time and effort. In the market, some SLA negotiation tools contain SLA

	templates used to initiate the negotiation process. Cloud service provider should know in advance on how to find a suitable ratio of payment and/or operational cost so as to create feasible SLA templates(Spillner & Schill, 2009).
Deliverable	**SLA Document** After negotiation, a comprehensive SLA document, held by both cloud service consumers and providers, should be put into place. SLA can be recorded into a normal document and customized later. Consumer organizations should pay attention to some important factors when creating SLAs, including(Cloud_Computing_Use_Case_Discussion_Group, 2010; IBM, 2010c; Raines & Pizette, 2010; Spillner & Schill, 2009): • Business level objectives: organizations must define why they want to use a cloud service. • Responsibilities of parties: within the SLAs, it is important to define corresponding responsibilities among different parities, including relationships with external parties and internal parties. For instance, in public cloud, providers will be responsible for running, maintaining services in SaaS and consumers will be responsible for the security of the sensitive data. In private cloud, IT department will be responsible for maintain and business departments will be responsible for classifying the data. • Business continuity/disaster recovery: consumers should ensure that providers maintain adequate disaster protections. Consumers usually use cloud as the backup of their in-house datacenters and perform cloud bursting (i.e. switchover when in-house data centers are unable to handle processing loads). Neither of the solutions will success unless providers have stable procedures. • Redundancy: consumers should consider how redundant the provider's systems are. This option will link to previous consideration. If CSP’s data center is redundant, then outage will be probably well controlled. • Maintenance: in cloud, providers are usually responsible for maintenance[10]. Consumers should know about the frequency of the maintenance and whether

[10] This situation is most applicable to public cloud services.

the maintenance will influence their applications running on top of the cloud. They should ask their providers whether they can use the updated services.

- Data location: data location is restricted. Consumers should ensure that their providers can guarantee the location of the data and keep the right to audit their providers.
- Data seizure: even though there have been well-published laws regarding seizure of data in hosting company, the multi-tenant nature of cloud computing will increase the possibility that other tenants will be affected because their services are running on the same server of the target consumer. Consumers should consider the laws that apply to the providers.
- Provider failure: when consumers make their contingency plans; they should consider the financial health of their providers. Besides, they should make clear the right of providers to access the delinquent or disputed services.
- Jurisdiction: consumers should understand local laws that apply to their providers. For example, CSPs can be based in a country that keeps the right to monitor any data or applications, which might not acceptable by your organization.
- Brokers and resellers: if the provider is a broker or reseller of cloud services, SLAs should clarity the liability and responsibility with regard to original providers and resellers.
- Clear definitions of charges and penalties (Amazon, 2010; Spillner & Schill, 2009).
- Data Inspection: Consumers should specify the right to obtain some data. For example, consumers want to acquire the underlying infrastructure data for their internal problems management. (Cloud_Computing_Use_Case_Discussion_Group, 2010; Grobauer & Schreck, 2010).
- Support: consumers should clarify the responsibility to support. For example, the internal help desk will handle the problems raised by the service module, providers' help desks will hand the problems regarding infrastructure. Not all SLA can be implemented automatically; therefore it is necessary to outline

	human interactions for the support. - Period: specify a valid period the SLAs will cover and the frequency of reporting.

4.6.2 Monitor compliance

Process Name	**Monitor compliance**
Description	After SLAs have been agreed upon, they have to be managed properly so that the parameters used to determine the performance of the service in contracts can be verified. Consumer organizations can assign one person to monitor and count the violations manually. However, as services and parameters grow within the organizations, this process will become difficult and time-consuming. Automated SLA monitoring tools can enhance the process through checking the messages, monitoring the performance, and registering the errors in real time. Two monitoring approaches are found in literature, namely proactive and reactive respectively. The first relies on triggering an action on a threshold below the service level to prevent from SLA violation. The later relies on trigging an action based on SLA violation. Warnings will be sent when a service is underperformed(Schepers, 2007).
Method	For monitor, what interests us is what metrics organizations should use to measure and monitor their providers and what functions the monitoring tools should possess. First, consumer organizations should define metrics to ensure that the cloud services comply with the legal regulations and the industry standards. Since detailed metrics depend on the nature of cloud computing and the requirements, it is impossible to list all the metrics. Yet there are some common metrics can be used as an guideline(Cloud_Computing_Use_Case_Discussion_Group, 2010), including: - Throughput: how quickly the service responds. - Reliability: how often the service is available. - Load balancing: when elasticity kicks in (new VMs are booted or terminated, for example). - Durability: how likely the data is to be lost. - Elasticity: the ability for a given resource to grow infinitely, with limits (the

maximum amount of storage or bandwidth, for example) clearly stated.

- Linearity: how a system performs as the workload increases.
- Agility: how quickly the provider responds as consumer's resource load scales up and down.
- Automation: what percentage of requests to the provider is handled without any human interaction?
- Customer service response times: how quickly the provider responds to a service request. This refers to human interactions required when something goes wrong with the on-demand, self-service aspects from cloud.

The metrics listed above are mostly applied to measure the quality of a service. Apart from the metrics, two more metrics should be considered for monitoring, namely usage and cost(Patel, ranabahu, & Sheth, 2009). Cost monitoring will highly depend on charging strategy from CSP. In 4.3.5, we have discussed some possible charging back strategies used in internal organization or private cloud. When using public cloud, cost per unit is usually provided in SLA. Together with actual usage information, organizations can audit the cost of the service.

Next ,some key functions that the monitoring tool should have, are outlined as follows :

- Indicate trend for different parameters: Most of the metrics from CSPs are the as-is data source such as transaction count and it is useful to provide some more insightful and contextual information through applying one or more algorithms to trim the coarse data. For instance, the tool can show the usage trend prediction based on the historical requests.
- Alert SLA violations and specify what is needed to be done during the violation: The tool should allow setting up thresholds for violation indication.
- Point out compliancy for customers during the violation as well as when the value is approaching the threshold, enabling relevant owners to take action.
- Calculate fee for a service.

Because there is a lack of standardization in cloud computing context, consumer organizations can consider introducing a middleware to monitor multiple cloud

	providers. As it is still difficult to set up a universal set of metrics to monitor across multiple cloud vendors, organizations can elicit the metrics from best practices in industry gradually.
Deliverable	**SLA report and alerts** The deliverable of this process should be about how SLAs are monitored. A best approach to indicate the results is through SLA reports and alerts. Generally, SLA reports are used to display the service performance on the service parameters for a specific timeframe. The reports can be linked to the parameters. For example, users can retrieve a "service availability report", "reliability report" and so on. All the services in relation to the parameter can enable a SLA parameter report. For each parameter, the following attributes should be included within a report: • Clear *period* for the report: how often is it going to be monitored? Monthly base, weekly base? • *The person* who is responsible for the report: even though adjustment and action can be taken in automated way, it is still necessary to assign one person to check for the report and gain insights for updating thresholds. • Trend indication for those parameters: this information will be very useful for organization to take action when there is violation. For example, financial penalties will indicate terminating one service or updating SLO. Sometimes this trend information will lead to no action when low performance is just temporary. In cloud, those reports can be generated by service providers and sent to the consumer organizations. In fact, consumer organizations can build up their own SLA monitoring mechanisms and compare the reports from their providers to prevent from deception. Another advantage of setting up their own monitoring mechanisms is to enable automating some reactions to the warnings and violations and integrating on-premise services and cloud services. For example, when the service from one of the provider is not available, organizations can switch to another service on-premise.

	When a parameter report causes warnings, it is important to consider: • Define an action value for metrics in SLA in order to trigger the actions. The actions will be taken when the actual value is below or above the threshold. • Define actions when a remedy process is triggered. For instance, send emails to the owners or redirect the requests to other traffic. • Ensure reverse action: this function enables users or services to get back to the normal situation.

4.6.3 Evaluate services

Process Name	**Evaluate services**
Description	This process is set up to evaluate the services and contracts. It evolves from compliance monitoring and should be performed after the services go into production for a while. The purpose of the process is to determine how the services work as a whole and whether they add values to the business as expected. From the evaluation, organizations can make decisions on what they should do with the services later. For public cloud, organizations can make decisions to terminate a contract, extend a service, switch to other suppliers, or add new virtual machines. For private cloud, some infrastructural change will be performed. For example, whether the organizations should continue with virtual automated resource provision and transformation.
Method	In 3.2.1 we have discussed how to calculate return of investment. The ROI calculate will cover the entire plan while the cost/benefit analysis discussed here will focus on one single service or one virtual instance. Determining the costs is believed to be important because benefits are usually intangible and hard to express in figures. For private cloud, costs will be divided into two, development costs and maintenance costs. The cloud enables developers to accelerate the whole development process and part of the maintenance can be automated as much as possible. Organizations can compare the costs to the costs for traditional similar services. For public cloud, costs will origin from the expense paid to the providers and internal support costs (e.g. the internal staff to support the service and maintenance cost for monitoring and governing technology). In SOA , Schepers proposes to evaluate service once or twice a year to make sure that the evaluated service is running for months on average (Schepers, 2007). The same

	principle can be applied to cloud service evaluation. For the benefits, since most of them belong to qualitative benefits. And those qualitative factors are usually used for analysis. This does not provide an easy way to make decision, yet manager with rich experience can tell the final decision whether to invest or not.
Deliverable	**Action Plan** During the evaluation process, problems regarding the individual service will be analyzed. A solution will be proposed to solve the problems, some of the possible actions of the solution will include: • Updating SLA parameters (Patel, et al., 2009). • Determining whether to terminate a service or an instance • Penalties should be executed when SLA cannot be met. For example, organizations can follow the charge back policy from public cloud service providers to get the credit back after a period of monitoring the violation of SLA from CSP. • Updating billing schemes for private cloud or public cloud within organizations

5 Governance-as-a-Service

We have discussed possible processes for cloud governance from the perspective of cloud consumer organizations. Tools and methods are identified for those processes. Some of the tools can be provided by CSPs directly together with their cloud offering. The cloud paradigm offers the opportunities for third parties to realize the governance solutions implement them as cloud offerings and provide them through Internet. Those solutions can be called as governance-as-a-service in general. This section will discuss whether those tools should be outsourced and whether they should be placed into cloud.

Benefits to apply cloud concept to implement governance technology is promising since it advocates resource sharing and consumers do not have to worry about maintenance so that they can focus on their core businesses. Nevertheless, the purpose of those cloud governance solutions is meant to protect regular cloud applications from intrusion and attack. When those guards are also provided through internet, or even implemented to support multi-tenant, one question will occur to customers that how safe those solutions are.

Answers to this question depend on type of the tools[11]. It will be appropriate to move testing tools into cloud. In fact, advantages of cloud testing services are not only limited to saving upfront cost on test server, it also provides a real-life simulated environment enabling better testing. Normally PaaS service provider will offer testing capability as part of software development lifecycle, for instance Windows Azure(Microsoft, 2011). This capability can be realized by third parties through extending the testing capability cross IaaS to SaaS. It can provide the opportunity for researchers to experience large-scale deployment of services across multiple continents(HP, 2011). Not only the cloud service but also regular on-premise service can utilize the testing capability.

When it comes to policy management tools, the answer should be cautious since policy enforcement gets involved with many security issues. Lang proposes a policy-as-a-service concept, emphasizing on policy configuration is provided as a subscription-based cloud service to application development (Lang, 2010b). In such a way, application developers and security experts can make use of those policy feeds without knowing details of the models. CSPs will take care of maintenance, modeling and update of

[11] In literature, governance-as-a-service mainly refers to services that make sure security and quality of services running in the cloud, testing tools are out of the scope. In this research, we include testing tools since testing is part of governance model.

policy. Whether consumer organizations should choose cloud-based authorization policy management services also relies on the inherent level of trustworthiness and reliability of the protected cloud applications. When applications themselves can be obtained in internet, attack on policy management service will direct to application they protect. There is no big difference using on-premise policy management service or cloud-based policy management service. Nevertheless, if the policy service is used to protect high security demand private cloud service, organizations should consider other more conservative protection mechanisms.

As we discussed before, policy enforcement point should be integrated into CSP cloud platform so that generated technical policies can automatically be enforced whenever cloud application are accessed. Where policy enforcement points are executed, alerts and incidents will be collected. Log and audit information will be provided to customers. Benefits of putting the collection function into cloud are obvious: incidents can be centrally analyzed for multiple cloud services together with other information. However, the information will be huge when log and audit is generated based on transaction or requests, increasing the cost to transfer the data. Consumer organizations have to take this into account when they decide to use governance-as-a-service solution.

Cloud computing is a metered service and requires to meter the usage through metrics. Both CSPs and consumer organizations can set up their own metrics to meter the usage. However, because the interests are conflicted between the two parties, the metrics and value will be controversial. In this circumstance, an third party should get involved to come up with a fair measurement(Cloud_Computing_Use_Case_Discussion_Group, 2010; Korn, Peltz, & Mowbray, 2009).

6 Model Validation

The proposed model is primarily derived from SOA governance and existing literatures on cloud computing. The goal of this paper is to provide practical guidelines so that organizations can be aware of the changes brought by cloud computing. They can adjust their current organizational structure, processes and introduce corresponding tools to support those processes. In order to validate the model, it is necessary to collect feedback from practice to ensure better alignment between theory and practice.

This chapter is further structured as follows: Section 6.1 will introduce how we setup the interviews and some information regarding the interviewees. Section 6.2 will present the findings on the interviews. The findings are mainly from the interview results while sometimes our opinions are considered. Section 6.3 will present some modification points on our model.

6.1 Interview setup

We have chosen qualitative approach for the validation. Case study is thought to be appropriate to get more feedback; nevertheless, it is impossible to conduct a case study due to immaturity of such projects in most of companies. Instead, we determine to conduct a series of interviews to provide a holistic view on current governance approaches and planed governance approaches in the future. It is expected to gain some insights from the interviews to see whether the processes and approaches or tools listed in our model are necessary and critical. If possible, other important processes can be added into the model.

Three types of qualitative interviews are mentioned in literature(Fontana & Frey, 2000), including:

a) Structured interview: A complete script is prepared beforehand and there is no room for improvisation.
b) Unstructured interview or semi-structured interview: incomplete script has created and there is a need for improvisation.
c) Group interview: two or more people are interviewed by one or more interviewers.

Semi-structured interview is considered for this research since questions will be outlined in order to match with the structure of our proposed model and there is a need to collect more inputs from the interviews in order to compensate for the gap in literature. We have formulated a question list in Appendix H for the interviews and the questions are in line with the governance domains in our model. During the interview section, some explanations will be added in order to make the questions clear.

Interviewees are from various industries, the common characteristic of all the interviewees is that they all have knowledge and experience on cloud directly. Some of them are getting involved with the core governance responsibilities. The services they are using include SaaS, PaaS, and IaaS. Some organizations are providers of those solutions. It is believed that their experience with various clients will provide a valuable insight on our research.

Detailed interview information is given in Appendix I. Table 9 lists some basic background information of the interviewees, cloud service type we have discussed with the interviewee, and their working organization relationship with those cloud services. Table 10 summarizes the key points from each interview, which can be found in Appendix I.

Interviewee from	**Experience**	**Discussion Cloud Service Type**	**Relation of organization with cloud services**
Printing company	Promoter and in charge of cloud prototype	365 office and Google Apps	Direct users of public SaaS cloud service
Centre4Cloud	Director of one knowledge centre on cloud computing in Netherlands	Public SaaS, PaaS and IaaS	Educate and promote cloud services to both suppliers and clients
Shell	Contractor in Shell, in charge of policy definition and contract negotiation on cloud service	Private and public SaaS applications	Direct clients of public SaaS cloud services
Mendix	Cofounder of the company	Public IaaS ,PaaS and SaaS	Client of public IaaS service Provider of PaaS service and SaaS service
Novay	Manager of Novay ICT institution	Public IaaS , PaaS and SaaS	Client of public IaaS and PaaS Provider of SaaS
Logica	Software architect on Azure Datacenter	Public PaaS (Microsoft Azure)	Clients of public PaaS. Providers of SaaS
EuroCloud	Vice President of EuroCloud	Public SaaS	Provider of SaaS certification program to client organizations

Table 9 Interview background

6.2 Findings

This section will present the main findings from the interviews.

Pay more attention to public cloud

Organizations should focus on public cloud services and private cloud services should be used to keep up with public ones. On the one hand, the potential benefits from public cloud services are huge. Not only that organizations can delegate their IT business to their suppliers and focus on their core business, but also the public cloud services can accelerate inter-organizational interaction and processes. On the other hand, as the control level of public cloud services is lower, it requires organizations to pay more attention to them. As for private cloud, interview results indicate that governance mechanisms for private cloud services are basically the same as traditional IT governance. The focus of private cloud services should be managing the evolution of internal IT from mundane data center to state-of-the-art “private cloud” so that they can live up to public cloud requirements such as ease of procurement and quality of services.

Ensure TCO is in place before cloud is introduced and start pilot projects on non-critical applications

Strategic plan will not change dramatically, adopting new technology should base on comprehensive business case analysis. In other words, organizations should have a way to calculate Total Cost of Ownership (TCO) in order to make sure the value of introducing cloud computing. Implementation of cloud from reality should follow an incremental adoption approach**,** starting from pilot projects on the non-critical applications to reduce the risks.

Cloud coordinator will facilitate cloud adoption

There is no specific cloud centre of excellent in most of organizations because cloud implementations are in its initial stage. However, the expert from Logica claims that coordination jobs done by cloud experts and the regular cloud meetings with various experts help him to be aware of most cloud issues and grab the essence of cloud quickly.

IT roles should shift to contract management and information management

Most of interviewees suggest that ownership of a cloud service will be going back to business departments. IT responsibility will decrease or shift to contract management and information management (e.g. data privacy, portability and interoperability). In reality, business departments usually bypass IT to subscribe their own services. Without principles or IT policies to guide business managers, IT will confront with difficulties in data integration or service interoperability in the future. Even though there is a trend indicating that cloud services will be oriented to an open environment, most of the organizations are still struggling with integration problems, especially with existing on-premise services. Contract managers can oversee the common organizational-wise services, ensure the whole value of those services, and be responsible for the charge back issues to business. The rest of the departments can decide and select their own services, nevertheless, they have to follow the standard or guidelines set by relevant governance council to ensure organization-wise consistency.

Testing security on cloud will be difficult

Testing is always an effective way to check the quality of services before they are deployed and executed. For SaaS services, client organizations will conduct the test against their customer/end-user requirements. Meanwhile, performance and security testing should be taken into account. However, the difficulties to test security of services increase from IaaS to SaaS. On the one hand, the control level of client organizations diminishes in the order of IaaS, PaaS and SaaS. On the other hand, more stakeholders will probably get involved, making the test difficult. The focus of security testing will probably move to contract and SLA evaluation and monitoring and rely on the suppliers to ensure the infrastructure security requirements.

Delegate incident management and low level configuration management to suppliers, take care of change management

PaaS and SaaS consumer organizations should delegate incident management to their suppliers since suppliers usually have better knowledge and skills and they will exert their best effort to solve the problems and keep their business. As a result, the responsibility of internal service desk will increase because it helps to bridge the relationship with customers and suppliers. Change management should be arranged by consumer organizations to handle business changes which are initiated by the organizations or their suppliers. Service providers should provide capabilities to support consumer organizations' change requirements. Consumer organizations can consider a change package in the contract to deal with the periodical business regulation changes.

Establish policy management processes internally and externally

Policy management is the least considered aspect according to the interviewees. In our discussion, policy mainly refers to security policy and performance policy. Some of the interviewees believe that policy management is only related to SaaS level. We do not agree with that because information security issues cover from IaaS to SaaS services usage. Design time policy (i.e. defining policy) is considered by most of the organizations, however, enforcing policies automatically seems impossible at the moment. As stated in our main text, policy enforcement in cloud depends on suppliers. Automatic policy enforcement in cloud is the ultimate goal. When it is not possible, manually policy enforcement to facilitate policy communication is still necessary. Three main sub-processes regarding policy management should be considered. First, business departments should put up with their data policy in accordance with business rules or probably laws so that contract managers can deal with the data properly. Second, IT department should define general policies and guidelines to navigate business departments on the usage of cloud. For example, how to choose cloud services, how to define their data or share their data to facilitate data integration. Third, contract managers should understand suppliers' policy and inform business departments when it is necessary. For instance, when there are some changes initiated by CSPs, contract managers should inform business departments to prepare something to be adaptive to the changes. .

Monitoring SLA can depend on third party organizations to avoid upfront investment

Adopting public cloud services is similar to outsourcing part of the services to suppliers. How to clarify responsibilities and ensure the value of cloud highly depends on the contract negotiation and SLA definition. We found out that all the interviewees emphasize the importance of contract or SLA management. In practice, most of the control mechanisms start from SLA management even though cloud governance technologies are in its infancy. Monitoring SLA becomes one of control mechanisms that consumer organizations can take. Nevertheless, whether they should implement SLA monitoring on their own is open to question. For one thing, SLA monitoring implementation requires upfront investment, increasing the cost to terminate the service. In addition, totally relying on the information sent by the providers will be not wise. Organizations can consider hiring third party such as KPMG, Eurocloud to check and audit the suppliers for them. Nevertheless, if SLA monitoring depends on untrustworthy parties, organizations have to establish another control mechanism to control over the third parties, which will make the monitoring more complicated.

Introduce a self-service portal and registry/repository to support governance

Even though most of the governance technologies regarding cloud governance are still in its infancy, we believe that relevant vendors should exert their effort to transit their products from existing SOA governance technologies to the cloud. One of the main products includes the registry/repository. It can provide instant on-demand access to the catalogue of all the services (e.g. internal and external services). Backed by the usage/policy monitoring and chargeback mechanisms, it is the key service that LoB and IT department, consumer organizations and providers use to share their information(e.g. pricing and product detail), enabling configuration, user access management and service delivery within consumer organizations.

Whether business continuity should delegate to suppliers depends on TCO

No matter what the suppliers guarantee, it is still possible that their services will fail. Traditionally, organizations will replicate services and data to prevent from downtime of the cloud services. However, if a service is already available on-premise and it requires people and resources to support the execution, what is the point to use public cloud services? How can cloud add value to the business? Some of the interviewees suggest that business continuity should be delegated to suppliers as well. Another option is that organizations can use multiple suppliers to mitigate the risk. The final decision should rely on TCO. In general, it is cheaper to use one supplier and multiple datacenters than multiple suppliers and multiple datacenters. In fact, all the solutions are used by organizations. Mendix uses multiple suppliers and builds its own datacenter because multiple suppliers will probably enlarge their business opportunities and building its own datacenter can compensate the risk to lose its business. Logica backs up the data on-premise to avoid failure of service providers. It is claimed that moving back the services to on-premise infrastructure won’t take a lot of time.

Evaluate services periodically to compensate lost and take actions

Consumer organizations should evaluate services against SLA or check the reports sent by third parties periodically. Sometimes immediate actions will need to be taken to ensure that the organizations can get the right compensation from their suppliers. For big companies such as Shell, evaluation results can be used as an input to negotiate service credits with their suppliers. When the worst thing happens, organizations can consider terminating the service.

Arrange exit plans to avoid vendor lock-in

In the case that organizations want to change suppliers or bring a service back in-house, an exit strategy should be made clear in the contract. Organizations should request the data back when terminating a service with their suppliers and they should consider the compatibility of the data with their on-site services or another suppliers' services they are about to move to. Client organizations should try to get the support permission from their suppliers to avoid some transition risks.

6.3 Modified process model

In general, our model covers the most important opinions from practice. We do not provide a thorough analysis with respect to different types of cloud for the sake of the limited space. However, we provide a relationship summary between types of cloud and the processes in our model in Appendix G. According to the findings, we have found some flaws in our generic process model. This section will work on those flaws and make some adjustments in our model.

First, in process 6 (i.e. assign responsible teams) we argue that when cloud services are highly separated, distributed approach can be taken into account. After interview with the experts, it turns out that it is more logical to adopt centralized governance approach to define some basic principles at the very beginning. Actually, even though services are highly separated, no one can predict that whether there is a need to integrate the services or data together in the future. If any business manager can subscribe any service without following instructions, integration of the services will probably become problematic in the future. Besides, the contract manager or CIO who take cares TCO for the whole organization for cloud services will have no idea on how many services some business departments have subscribed with and which suppliers they have contracts This will increase the difficulty to merge the same functional services from several suppliers.

Second, we propose to add one process in service lifecycle management, which is "create service support models". This process is mainly about establishing a service desk to deal with the problems encountered by business departments or end-users. Service desks from client organizations should have intimate connections with service desks from their suppliers. Organizations can consider having their own experts to handle some problems which are separated from suppliers' infrastructure. For instance, service desks setup by PaaS providers have to solve the problems regarding the service modules delivered to the clients. When the problems are related to infrastructure from IaaS providers, PaaS providers should forward them to their IaaS suppliers. The whole process requires the service desk to hold a good classification of questions in relation to their own services and their suppliers'.

Third, two processes should make explicit in SLA management section. They are “delegate incident management” and “create exit plans”. In the process of “delegate incident management”, client organizations should make clear in their contracts that providers should take care of incident management in their organizations. When the incidents are escalated into problems and lead to changes regarding their service provisions, the providers should inform consumer organizations so that they can prepare for the changes. In the process of “create exit plans”; consumer organizations should specify in the contract that suppliers should provide necessary exit supports for them. For instance, suppliers should support the data transition from one format to another format without damaging the data. In the exit plans, it would be better to make a list of possible candidates which are compatible suppliers’ or probably their own datacenters.

Fourth, a process to manage suppliers should be placed into strategic plan section. One job for this process includes reviewing all the suppliers, their services and TCO regarding those services as a whole. CIO or the service manager can consider eliminating some suppliers for the same services they have provided. Another concern for this process is to unify internal and external control mechanisms. We have mentioned that some of the mechanisms will be delegated to third parties or service providers. The organization will probably be responsible for some control processes towards their own customers. How the organization makes those control mechanisms consistent should be considered. For instance, incident management activities which they have delegated to providers and the one they have to take care for their consumers.

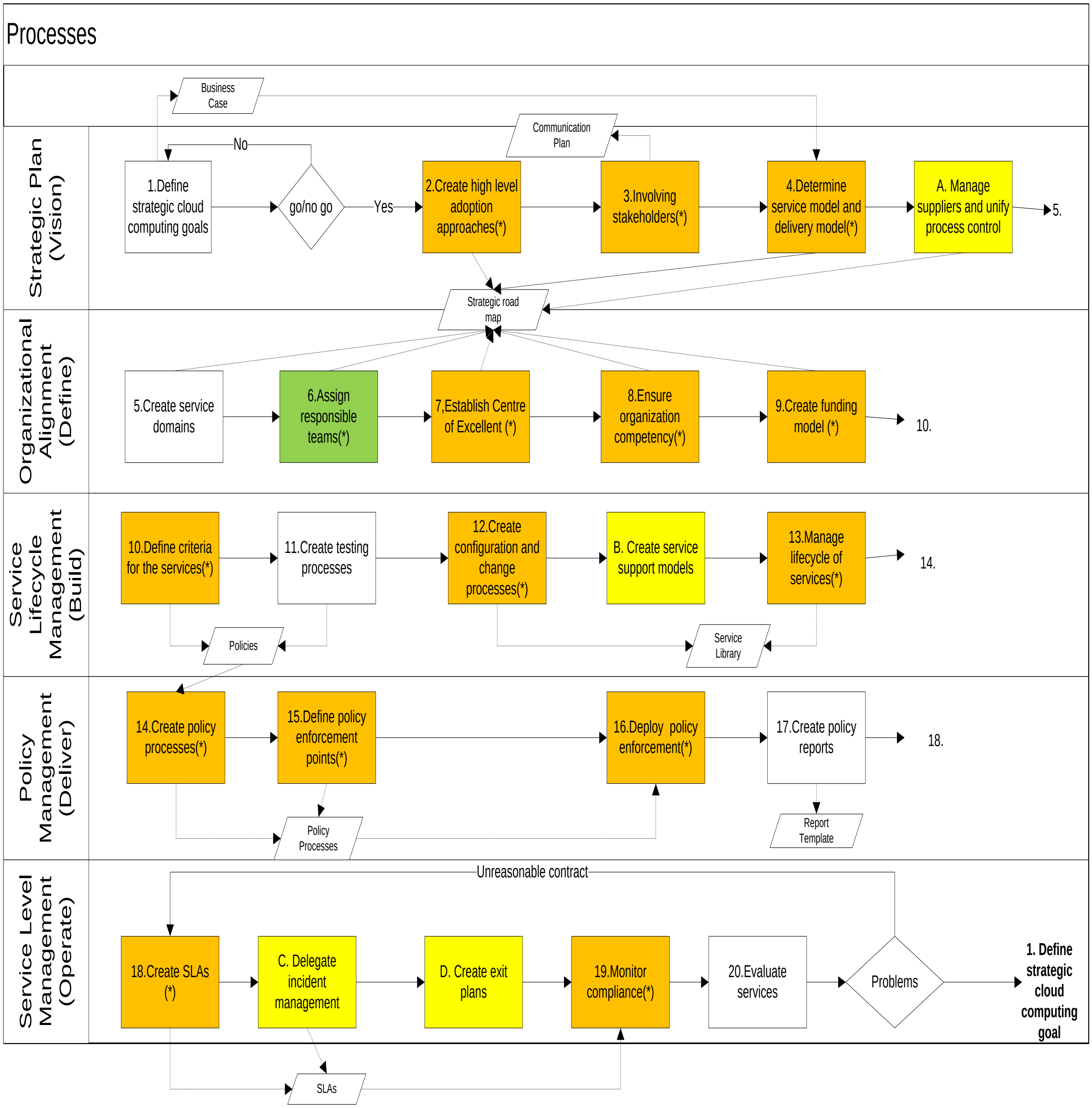

Processes
Business Case
Communication Plan
Strategic Plan (Vision)
1.Define strategic cloud computing goals
No
go/no go
Yes
2.Create high level adoption approaches(*)
3.Involving stakeholders(*)
4.Determine service model and delivery model(*)
A. Manage suppliers and unify process control
5.
Strategic road map
Organizational Alignment (Define)
5.Create service domains
6.Assign responsible teams(*)
7,Establish Centre of Excellent (*)
8.Ensure organization competency(*)
9.Create funding model (*)
10.
Service Lifecycle Management (Build)
10.Define criteria for the services(*)
11.Create testing processes
12.Create configuration and change processes(*)
B. Create service support models
13.Manage lifecycle of services(*)
14.
Policies
Service Library
Policy Management (Deliver)
14.Create policy processes(*)
15.Define policy enforcement points(*)
16.Deploy policy enforcement(*)
17.Create policy reports
18.
Policy Processes
Report Template
Service Level Management (Operate)
Unreasonable contract
18.Create SLAs (*)
C. Delegate incident management
D. Create exit plans
19.Monitor compliance(*)
20.Evaluate services
Problems
1. Define strategic cloud computing goal
SLAs

Figure 25 Modified Lifecycle Process Model for Cloud Governance

🟨 **New process**

🟩 **Modified process**

🟧 **Original marked process**

7 Conclusion and further research

7.1 Research result

The main objective of the research project is to come up with a generic process model for cloud governance that can be applicable to all types of cloud. In chapter 1 we come up with five research questions which are formulated to answer the main research question “How can cloud computing service consumers implement cloud governance within their organizations?” This section we will look back to those questions. We believe that by addressing those questions, the main objective of the research has been met.

What are the activities needed to control cloud computing?

Based on the literature study and interviews from practice, a process model with five areas governance focus has been formulated to control over cloud computing within consumer organizations. For each area, a small amount of activities have been identified. In practice, those processes can be further broken down into small steps. Some processes should be customized to suit to the organization context. A summary of governance methods with all the activities can be found in Figure 25.

The activities within the model range from high level strategic planning activities to technology-oriented activities (e.g. “create testing processes”). Both IT people and business man should understand the activities to enable better coordination within the organization(s).

How can cloud governance be tailored to different types of clouds?

Cloud computing has different service models and deployment models (see 2.2). The processes we have identified are meant to be applicable to all type of cloud services. Nevertheless, there are some differences among the types of services, leading to slightly different activities within the processes. We do not have a section to discuss this topic specifically. Nevertheless, we do consider how the service types will influence those processes when analyzing the processes. A brief summarization can be found in Appendix G.

The control level between consumer organizations and CSPs regarding different types of cloud is the main factor influencing the processes. Because public suppliers and the consumer organizations have to share the control, leading to a series of coordination activities between them, including incident management, service support, policy enforcement, and configuration and change management. As the control level also differ when it comes to different cloud service models (i.e. SaaS, PaaS, IaaS), some processes should be adaptive as well. For instance, the configuration items regarding different service model should be different, too.

In general, we believe the processes we have identified can be used for various cloud types mentioned in Section 2.2. Small adaption is still needed for a specific type of cloud.

What tools can support cloud governance processes?

This research question aims to search for scientific tools or software to support the processes in our model. In such a way that governance activities can be executed more easily. Some of the tools have already been available in IT governance or SOA governance field. Those tools can be reused or adjusted for cloud computing.

However, because of the immatureness of cloud governance tools and market, most of the tools do not completely support the whole processes. From the interviews we find out that tools which most of organizations adopt for cloud currently are the SLA and usage monitoring tools. Big organizations such as Shell have more control tools available in their organizations ranging from strategic decision to SLA monitoring tools. As for small companies, they have not investigated many tools for selecting their suppliers or supporting high level decision making. Most of the time, small companies prefer to use the tools provided by their cloud suppliers and rely on suppliers' information. They seldom audit their provider's information unless this will influence their core business.

Policy management tools are barely used by most of the organizations. One reason is that those tools are still under investigation, especially for run-time policy enforcement in cloud. Another reason is that centralized policy management is hard to implement within organizations. Meanwhile, many organizations overlook the importance of policy process and do not pay attention to increasing the awareness to share their policies among the organizations.

The key tools to support Lifecycle management should be registry/repository tools. These tools can facilitate the information sharing between consumers and providers, LoB and IT department, ensuring the behavior of users and services. Since these tools are still in their infancy, a new opportunity for the vendors is to investigate how to transit the exiting SOA governance tools to cater for the cloud setting.

Should organizations outsource governance?

In chapter 5, we have discussed whether the governance tools should be outsourced and whether they should be placed into cloud, in which testing tools, policy tools and SLA tools have been analyzed. Obviously there are a lot of advantages to put testing the tools into cloud. Whether policy tools should be put into cloud or Internet depends on the accessibility of the applications and the organizational security requirements. SLA monitoring tools can be delegated directly to the cloud providers; however, because of the conflicted interested between consumer organizations and providers, an authority party should be considered to ensure the fairness. Here we emphasize the authority party instead of normal third party. Otherwise consumer organizations will have to create another control mechanism to oversee their control parties. No matter what choice consumer organizations have made, it is necessary for them to consider how to make the internal and external control mechanisms consistent.

How can we test the proposed model?

The interviewees we have contacted include CIO, Architect, Contractor and Scholars who have direct experience on cloud computing. Some of them offer direct cloud services to their clients and have rich experiences on how their clients deal with control activities. Some of them are the key stakeholders in the governance activities. Some of them offer third party governance solutions to cloud consumer and provider organizations. The services cover IaaS, PaaS, and SaaS. Private and public cloud services are involved but the focus will lean to public services. Individual interview details can be found in Appendix I and an overview summary on all the interviews are summarized into Table 10. Relevant findings from the interviews are listed in section 6.2.

7.2 Limitations and further researches

This study has several limitations. First of all, scope of the study is too broad. It includes almost all types of cloud services (e.g. different service models and deployment models). Because of the broad scope and the limited time frame, we have to keep the research at a higher level rather than discuss each type of service in detail. In addition, when the model is designed for many types of services, it is not easy to generalize the processes. And the research perspective has also been influenced when so many types of services are involved. Sometimes suppliers can be the clients of lower stack of cloud services. For instance, PaaS provider can be client of IaaS services and SaaS providers can be clients of PaaS providers.

Second, how the model is applied to different organizations is not considered in our model. Actually, not every organization requires the same level of governance. Even for the same organization, governance requirements will change. In order to make sure that organizations can implement the governance model gradually, a maturity model with criteria to define the maturity level for each process should be considered for further research.

Third, there is a lack of linkage between the roles and processes in our model. Further research can consider adding the linkage to make governance responsibility more clear. Actually, not all the roles are needed for each type of service model. Researchers can narrow down the scope to a specific type of cloud and identify the roles with respect to the type of cloud.

Fourth, governance can mean different things to different people. This thesis has tried to give a broad view on cloud governance in relation to organization issues and extended the SOA governance methodology to cloud. The final governance areas have been scoped to five main areas. Because of the immaturity of the concept on cloud governance, some parts need to be researched further in the future. Researcher can take the auditor perspective to explore the contents to audit suppliers. Corresponding information on this topic include COBIT framework, the audit program on cloud computing from ISCASA and the SaaS audit certification from EuroCloud. The last section of our model has mentioned about auditing but further investigation is still required.

References

Agilepath_Corporation. (2011). *Exploring the cloud governance lifecycle: Accelerating the transition to a cloud-centric leadership organization*.

Almaden_System. (2010). Cloud adoption strategies. from http://www.almadensystems.com/index.php?option=com_content&view=article&id=51:cloud-adoption-strategies&catid=35:cloud-computing&Itemid=27

Amazon. (2010). Amazon EC2 service level agreement. from http://aws.amazon.com/ec2-sla/

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., et al. (2010). A view of cloud computing. *Commun. ACM, 53*(4), 50-58.

Australian_Government. (2011). Cloud computing stratigic direction paper: Opportunities and applicability for use by the Australian Government. Retrieved from http://www.finance.gov.au/e-government/strategy-and-governance/docs/draft_cloud_computing_strategy.pdf

Benedetto, C. (2006). SOA and integration testing: the end-to-end view Available from http://webservices.sys-con.com/read/275057.htm

Bentley, Y. (2010). Cloud computing: Is ITIL still relevant? . http://h30501.www3.hp.com/t5/IT-Service-Management-Blog/Cloud-computing-Is-ITIL-still-relevant/ba-p/3663

Bieberstein, N., Bose, S., Fiammante, M., Jones, K., & Shah, R. (2005). Service-Oriented Architecture Compass - Business Value, Planning, and Enterprise roadmap Available from http://my.safaribooksonline.com/book/software-engineering-and-development/soa/0131870025

Binning, D. (2009). Top five cloud computing security issues. from http://www.computerweekly.com/Articles/2010/01/12/235782/Top-five-cloud-computing-security-issues.htm

Brown, W. A., Moore, G., & Tegan, W. (2006). *SOA governance - IBM's approach*.

CA_Technology. (2011). Survey Shows Cloud Computing Elevating the Role of IT: Focus on Business Strategy and Innovation. Retrieved from http://www.ca.com/news/Press-Releases/na/2011/Survey-Shows-Cloud-Computing-Elevating-the-Role-of-IT.aspx

Castaldini, F. (2008). *SOA Governance and CentraSite: Ensuring SOA success with effective , automated control throughout the lifecycle*.

CBDI. (2008). SOA Governance: Challenge or Opportunity. *CBDI Journal*.

Cheliah, P. (2011). SOA Governance in the Cloud *SOA magazine*.

Cisco. (2010). *Managing the Real Cost of On-Demand Enterprise Cloud Services with Chargeback Models*.

Cloud_Computing_Use_Case_Discussion_Group. (2010). Cloud Computing Use Cases. Retrieved from http://cloudusecases.org/Whitepaper_V4_Draft_2.pdf

Cloud_Security_Alliance. (2009). Security Guidance for Critical Areas of Focus In Cloud Computing V2.1. Retrieved from http://www.cloudsecurityalliance.org/csaguide.pdf

COBIT. (2005). COBIT 4.0.

Colville, R. J., & Spafford, G. (2010). *Top Seven Considerations for Configuration Management for Virtual and Cloud Infrastructures*: Gartner RAS Core Research

Creswich, B. (2010). *IT/IM Cost Allocation and Chargeback in Federal Cloud computing Environment* Chartis Consulting Corporation

de Leusse, P., Dimitrakos, T., & Brossard, D. (2009, 6-10 July 2009). *A Governance Model for SOA.* Paper presented at the 2009 IEEE International Conference on Web Services.

Delioitte. (2006). The Enterprise Value Delivery Framework

DevCentral. (2008). Governance in the Cloud. http://devcentral.f5.com/weblogs/macvittie/archive/2008/09/09/3600.aspx

Dillon, T., Chen, W., & Chang, E. (2010, 20-23 April 2010). *Cloud Computing: Issues and Challenges.* Paper presented at the 24th IEEE International Conference on Advanced Information Networking and Applications (AINA).

Dinoor, S. (2010). Privileged identity management: securing the enterprise. *Network Security, 2010*(12), 4-6.

Dow, M. (2007). *Criteria for designing quality enterprise services definitions.*

Erl, T. (2005). Service-Oriented Architecture: Concepts, Technology, and Design

Eucalyptus. (2011). Cloud IT Roles. from http://open.eucalyptus.com/learn/cloud-it-roles

Eurocloud. (2011). from www.eurocloud.org

Farrell, R. (2010). Securing the Cloud-Governance,Risk, and Compliance Issues Reign Supreme. *Information Security Journal: A Global Perspective, 19*(6), 310-319.

Fontana, A., & Frey, J. H. (2000). The interview: from structured questions to negotiated text. In Y. S. Lincoln (Ed.), *Handbook of qualitative research* (pp. 645-672).

Grobauer, B., & Schreck, T. (2010). *Towards incident handling in the cloud: challenges and approaches*. Paper presented at the Proceedings of the 2010 ACM workshop on Cloud computing security workshop.

Guo, Z., Song, M., & Song, J. (2010). *A Governance Model for Cloud Computing*. Paper presented at the Management and Service Science (MASS).

Head, M. R., Sailer, A., Shaikh, H., & Viswanathan, M. (2009). *Taking IT Management Services to a Cloud*. Paper presented at the 2009 IEEE International Conference on Cloud Computing.

Hojaji, F., & Shirazi, M. R. A. (2010, 9-11 July 2010). *AUT SOA governance: A new SOA governance framework based on COBIT.* Paper presented at the Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on.

Hollis, C. (2011). What CIOs Really Want to Know about Cloud. http://chucksblog.emc.com/chucks_blog/2011/02/what-cios-really-want-to-know-about-cloud.html

Hondo, M., Portier, B., & Potepan, F. (2008). SOA Policy Management. Retrieved from http://www.redbooks.ibm.com/abstracts/redp4463.html

HP. (2011). HP Labs cloud-computing test bed: Technical overview. from http://www.hpl.hp.com/open_innovation/cloud_collaboration/cloud_technical_overview.html

Hurley, J. (2010). Cloudy With a Chance of Configuration Management. Retrieved from http://www.ca.com/files/WhitePapers/dy-with-a-chance-of-config-management_229535.pdf

IBM. (2010a). Cloud Service Design. https://www.ibm.com/developerworks/mydeveloperworks/blogs/c2028fdc-41fe-4493-8257-33a59069fa04/entry/chapter_9_cloud_service_design5?lang=zh

IBM. (2010b). Dispelling the vapor around cloud computing: Drivers, barriers and considerations for public and private cloud adoption. Retrieved from http://public.dhe.ibm.com/common/ssi/ecm/en/ciw03062usen/CIW03062USEN.PDF

IBM. (2010c). Review and summary of cloud service level agreement. from http://www.ibm.com/developerworks/cloud/library/cl-rev2sla.html?ca=drs-

IBM. (2011a). SOA Governance and Service Lifecycle Management. from http://www-01.ibm.com/software/solutions/soa/gov/

IBM. (2011b). Tivoli Service Automation Manager: Automate requesting, deployement, monitoring and management of cloud computing services. from http://www-01.ibm.com/software/tivoli/products/service-auto-mgr/

IDC. (2008). IT Cloud Services User Survey, pt.2: Top Benefits & Challenges. http://blogs.idc.com/ie/?p=210

ISACA. (2009). *Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives*.

Keen, M., Adamski, D., Basu, I., Chilcott, P., Eames, M., Endrei, M., et al. (2007). *Implementing Technology to Support SOA Governance and Management* IBM.

King, T. M., & Ganti, A. S. (2010, 6-10 April 2010). *Migrating Autonomic Self-Testing to the Cloud.* Paper presented at the Third International Conference on Software Testing, Verification, and Validation Workshops (ICSTW).

Korn, A., Peltz, C., & Mowbray, M. (2009). *A Service Level Management Authority in the Cloud*.

La, H., & Kim, S. (2009). A Systematic Process for Developing High Quality SaaS Cloud Services. In M. Jaatun, G. Zhao & C. Rong (Eds.), *Cloud Computing* (Vol. 5931, pp. 278-289): Springer Berlin / Heidelberg.

Lang, U. (2010a). *OpenPMF SCaaS: Authorization as a Service for Cloud & SOA Applications*. Paper presented at the 2nd IEEE International Conference on Cloud Computing Technology and Science.

Lang, U. (2010b). Security Policy Automation: Improve Cloud Application Security ROI. *ISSA Journal*

Layer7. (2011). *Steer Safely into the Clouds: why you must have cloud governance before you move your apps*.

Linthicum, D. S. (2009). Cloud Computing and SOA Convergence in Your Enterprise

Litoiu, M., & Litoiu.M. (2010). *Optimizing Resources in Cloud, a SOA Governance View*. Paper presented at the Proceedings of the 2010 Workshop on Governance of Technology, Information and Policies.

Logica. (2010). from http://www.logica.com/

ManageEngine. (2011). Four Keys for Monitoring Cloud Services Retrieved from http://www.manageengine.com/products/applications_manager/four-keys-for-monitoring-cloud-services-whitepaper.html

Marks, E. A., & Lozano, B. (2010). *Executive's Guide to Cloud Computing* New Jersey: John Wiley & Sons Inc.

Mather, T., Kumaraswamy, S., & Latif, S. (2009). Cloud Security and Privacy

Mendix. (2011). from www.mendix.com

Menken, I., & Blokdijki, G. (2009). Cloud Computing Certification Kit Specialist: Platform Management & Storage Management

Microsoft. (2010). Cloud Governance. from http://azuredecisions.com/2010/06/10/cloud-governance/

Microsoft. (2011). Visual Studio 2010 and Windows Azure: Test your services. from http://www.microsoft.com/showcase/en/us/details/f7839243-aace-4300-bb50-32bfbdc31da3

Mimecast. (2009). Cloud Computing Adoption: survey results. from http://www.continuitycentral.com/news04991.html

Morrison, K. W. (2010). Technologies for Enforcement and Distribution of Policy in Cloud Architecture. In N. Antonopoulos & L. Gillam (Eds.), *Cloud Computing: Principles, Systems and Applications* (pp. 305-325): Springer.

Nadhan, E. (2004). Service-Oriented Architecture: Implementation Challenges. *Microsoft Architecture Journal*.

NIST. (2009). The NIST Definition of Cloud Computing. Retrieved from http://csrc.nist.gov/groups/SNS/cloud-computing/

Novay. (2011). from www.novay.nl

O'Gara, M., White, E., Rajan, S. S., Roman, P., & MacVittie, L. (2009). SOA software Extends IBM WebSphere Service Registry Repository:SOA in the cloud *Cloud Computing Journal*. Retrieved from http://cloudcomputing.sys-con.com/node/1214819

O'Neill, M. (2009a). Connecting to the cloud, Part 1: Leverage the cloud in applications. Retrieved Nov. 9, 2010, from http://www.ibm.com/developerworks/xml/library/x-cloudpt1/index.html

O'Neill, M. (2009b). Connecting to the Cloud, Part 3: Cloud governance and security. from http://www.ibm.com/developerworks/xml/library/x-cloudpt3/

OCG. (2011). Service V Model. from http://itsm.certification.info/servicev.html

Open_Cloud_Standards_Incubator. (2010). Architecture for Managing Clouds.

Ovum. (2010). *Cloud governance: an overview*.

Patel, P., ranabahu, A., & Sheth, A. (2009). Service Level Agreement in Cloud Computing. Retrieved from http://knoesis.wright.edu/library/download/OOPSLA_cloud_wsla_v3.pdf

Peterson, G. (2010). Don't Trust. And Verify: A Security Architecture Stack for the Cloud. *Security & Privacy, IEEE, 8*(5), 83-86.

Plummer, D. (2010). *Cloud Governance*: Gartner.

Progress_Software. (2005). Why runtime governance is critical for SOA: a SOA Primer. from http://www.actional.com/resources/whitepapers/

Raines, G., & Pizette, L. (2010). *A Decision Process for Applying Cloud Computing in Feferal Environments*.

Rajan, S. S. (2010). Cloud Enterprise Architecture and TOGAF. from http://cloudcomputing.sys-con.com/node/1621013

Rimal, B. P., & Choi, E. (2010). *A Conceptual Approach for Taxonomical Spectrum of Cloud Computing.* Paper presented at the Ubiquitous Information Technologies & Applications, 2009. ICUT '09. Proceedings of the 4th International Conference, Fukuoka

Riungu, L. M., Taipale, O., & Smolander, K. (2010, Nov. 30 2010-Dec. 3 2010). *Research Issues for Software Testing in the Cloud.* Paper presented at the Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on.

Rizwan, A., & Lech, J. (2010). Triangulation Theory: An Approach to Mitigate Governance Risk in Clouds. Retrieved from http://salsahpc.indiana.edu/CloudCom2010/Poster/cloudcom2010_submission_153.pdf

Schepers, T. (2007). *A Lifecycle Method for Service Oriented Architecture Governance.* University of Twente, Enschede.

Scott, D., & Colville, R. J. (2011). *Provisioning and Configuration Management for Private Cloud Computing and Real-Time Infrastructure*: Gartner RAS Core Research.

Settle, M. (2010). Cloud Computing: How to Craft a Smart Chargeback Strategy. from http://www.cio.com/article/641583/Cloud_Computing_How_to_Craft_a_Smart_Chargeback_Strategy

Shan, T. (2010). Cloud Computing Maturity Model from http://cloudonomic.blogspot.com/2010/03/cloud-computing-maturity-model-cm2.html

Shell. (2011). from www.shell.com

SOA_CoE_Core_Team. (2010). *Service Oriented Architecture (SOA) Governance Model*. Retrieved from http://www.ftb.ca.gov/aboutFTB/Projects/ITSP/SOA_Governance_Model.pdf.

Spillner, J., & Schill, A. (2009). *Dynamic SLA Template Adjustments Based on Service Property Monitoring*. Paper presented at the Proceedings of the 2009 IEEE International Conference on Cloud Computing.

The_Open_Group. (2009). SOA Governance Framework.

Vael, M. (2010). Cloud Computing An insight in the Governance & Security aspects. Retrieved from http://www.isaca.org/Groups/Professional-English/information-secuirty-management/GroupDocuments/Across%20Cloud%20Computing%20governance%20and%20risks%20May%202010.pdf

van de Dobbelsteen, R. (2007). *Security in Service-Oriented Architecture.*

Vordel. (2010). Cloud Governance in the 21st Century. Retrieved from http://www.vordel.com/downloads/whitepaper_csb.pdf

Waggener, S. (2010). Cloud computing - The future and challenges of IT shared services from http://inews.berkeley.edu/articles/Apr-May2010/cloud-computing-EQ

Wang, L., Laszewski, G. v., Younge, A., He, X., Kunze, M., Tao, J., et al. (2010). Cloud Computing: a Perspective Study. *New Generation Computing 28*(2), 137-146

webMethods. (2006). SOA Governance: Enabling Sustainable Success with SOA. Retrieved from http://www.cioindex.com/nm/articlefiles/44428-SOA_Governance.pdf

YGL_Life. (2011). Small-Mid Enterprises prefer public clouds. from http://yglwinston.com/post/3180644807/small-mid-enterprises-sme-prefer-public-clouds

Yi, W., & Blake, M. B. (2010). *Service-Oriented Computing and Cloud Computing: Challenges and Opportunities*. Paper presented at the Internet Computing, IEEE.

Appendices

Appendix A: Definition of Cloud Governance from Literature

Articles or Authors	**Definitions**
(Guo, et al., 2010)	“the processes used to oversee and control the adoption and implementation of a cloud-based service in accordance with recognized policies, audit procedures and management policies”
(O'Neill, 2009b)	“applying policies to the use of cloud services”
(Cloud_Computing_Use_Case_Discussion_Group, 2010)	“the controls and processes that make sure policies are enforced”
(Microsoft, 2010)	“Governance in the Cloud is about defining policies around managing the above factors [availability, security, privacy, location of cloud services and compliance etc.] and tracking/enforcing the policies at run time when the applications are running.”
(Agilepath_Corporation, 2011)	“the decision making processes, criteria and policies involved in the planning, architecture, acquisition, deployment, operation and management of a Cloud computing capability.”

Appendix B: Collection of Cloud Governance Problems from Literature

Source	Categories	Description
(Vael, 2010) (Guo, et al., 2010) (Binning, 2009) (Microsoft, 2010) (Cheliah, 2011)	Compliance to laws or standards	- Locations of the services/data are need to control to ensure they are compliant to legal and business regulations.
(Binning, 2009) (Guo, et al., 2010) (Linthicum, 2009)	Hard to estimate the risks of cloud computing	- Companies do not hold a holistic view of risk regarding cloud computing and lack of approach to assess those risks
(Linthicum, 2009) (Guo, et al., 2010)	Consequences of changing services	- Change of service will incur unexpected results if dependency of services or components is not well defined and recorded. - Unexpected access service and change service will cause major business loss.
(Linthicum, 2009) (Bentley, 2010) (Guo, et al., 2010) (Vael, 2010) (Microsoft, 2010)	Ensuring quality of the services	- Quality of the services such as performance, availability and security of the services are needed to carefully monitor to ensure the business value, especially when the services are out of control of organizations. - Lack of testing capability regarding cloud services. - Lack of capability to monitor composite services from different sources/CSPs, it becomes more complex when services are outside boundary of organizations.
(Bentley, 2010) (Hollis, 2011) (ManageEngine, 2011)	Aligning organizations with the cloud	- Aligning organizations with strategic goals is not changed in cloud setting. - Changes on how services are charged and how costs are allocated within the organization; funding models is moving from project-based to pool-based.

		- Inability to identify which service should move to cloud. - Inability to determine when to add/remove cloud services.
(Hollis, 2011) (Linthicum, 2009) (Dinoor, 2010)	Aligning organizations with the cloud	- Empower roles and responsibilities to facilitate the cloud computing adoption might be emergent. - Communication requires aligning with current existing business unit as well as IT experts on the field.
(Bentley, 2010) (Vael, 2010) (Cheliah, 2011) (Menken & Blokdijki, 2009)	Cooperate with suppliers	- Require renewing effort in supplier management processes - Lack of communication regarding the change, events management initiated from CSPs. - Business demand estimation need to cooperate with supplier and help to create the right capacity of the service in time - Service Level Agreement should be clear defined to ensure change requests will react within a limited time frame. - It is difficult to enforce policies in a remote public cloud.
(Dinoor, 2010) (Vael, 2010)	Evaluate Cloud Service Providers	- Evaluate the processes and policies which the service providers define to ensure the consistence with internal service and security processes with the organization. - Ensure that CSPs have put the privacy control in place and demonstrate the ability to prevent, detect, and react to the breaches in timely manner. - Ensure that CSPs have the effective and robust security controls assuring information from their consumers. Ensure that the organization can rely on

		the controls to secure against the unauthorized access, change and destruction. - Ensure that CSPs are doing the "right" thing through third party certification such as third-party or service audit reports.

Appendix C: Solution Areas for Cloud Governance

Solution Area	Description	Source
Strategic Planning	Set out goals which cloud computing have to achieve. Select high level approaches for implementation, top down (business) or bottom-up (technology). Involve with stakeholders from IT and business to agree on the direction. Select services and determine proper service delivery models through workload. Create pilot studies for impact analysis.	(Schepers, 2007) (Ovum, 2010) (IBM, 2010b) (Marks & Lozano, 2010)
Organizational alignment	Make changes on organizational structure to adapt to cloud computing. Require creation of a centre of excellent as SOA to ensure organization-wise cooperation and decision making. New cost allocation for cloud services should be changed within an organization. New mechanisms are needed to define who pays, own and maintain the services.	(Ovum, 2010) (Australian_Government, 2011) (Bentley, 2010) (Creswich, 2010) (Schepers, 2007)
Service Lifecycle Management	This section will focus on individual service, considering the processes from acquisition or creating one service to the termination of the service. Topic such as change management, versioning, configuration management, testing etc. will be discussed. The lifecycle management will concentrate on the design time processes. The processes should be adjusted to meet the characteristics of cloud such as flexible and	(Ovum, 2010) (Linthicum, 2009) (Australian_Government, 2011) (Schepers, 2007) (Cheliah, 2011)

	virtualized. A central placeholder for developer/consumer to view services and associated processes should be established.	
Policy Management	This section is about designing and creating policies to manage usage of the services. Policies from cloud can include internal organizational policies and policies defined by public CSPs. Policy management in SOA relies on design-time and run-time infrastructure tools to define and enforce policies. Real time policy enforcement is critical, ensuring the behavior of services during the runtime and reducing the risks. In cloud, public CSPs should provide capability to allow developers/consumers to discover services and its associated policies as well as enforce their policies. Governance tools such as registries/repositories should support synchronization between internal and external registries and repositories to get the updated service lists and relevant information. New processes such as mapping internal and public policies should be created to increase the reusability of policies and facilitate improving the policy federation function of the registry and repositories tools. Organizations should create policy reports to improve policies and relevant activities. It would be better to set up automatic reports or a	(Ovum, 2010) (Schepers, 2007) (Open_Cloud_Standards_Incubator, 2010) (Guo, et al., 2010) (Microsoft, 2010) (Marks & Lozano, 2010) (Lang, 2010a)

	dashboard to notify relevant stakeholders in time. Policies and its relationship to the services should be stored into the registry and repositories tools for an easy administration.	
SLA Management	SLA is a contract between cloud service consumers and providers. SLA management enables consumer organizations to ensure their benefits and the value of cloud services through legitimate contracts. Within the management, consumer organizations can set up some monitoring mechanisms to prevent from reception of their suppliers. Sometimes, consumer organizations can establish their own monitoring tools to leverage the internal and external cloud services. Evaluation will be conducted periodically in order to ensure the value of the services provided by their suppliers.	(Australian_Government, 2011) (Schepers, 2007) (Vael, 2010) (Creswich, 2010) (Guo, et al., 2010) (Farrell, 2010)

Appendix D: Centralized and Distributed Governance Model from SOA

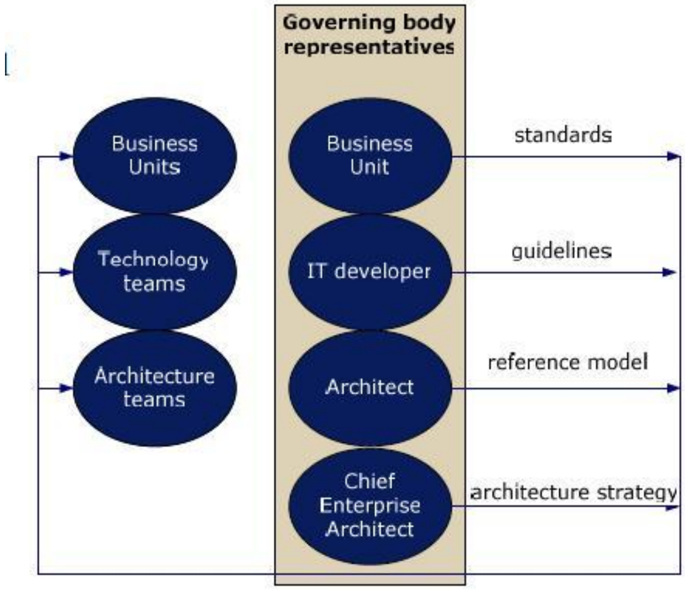


Figure 26 Centralized Governance Model

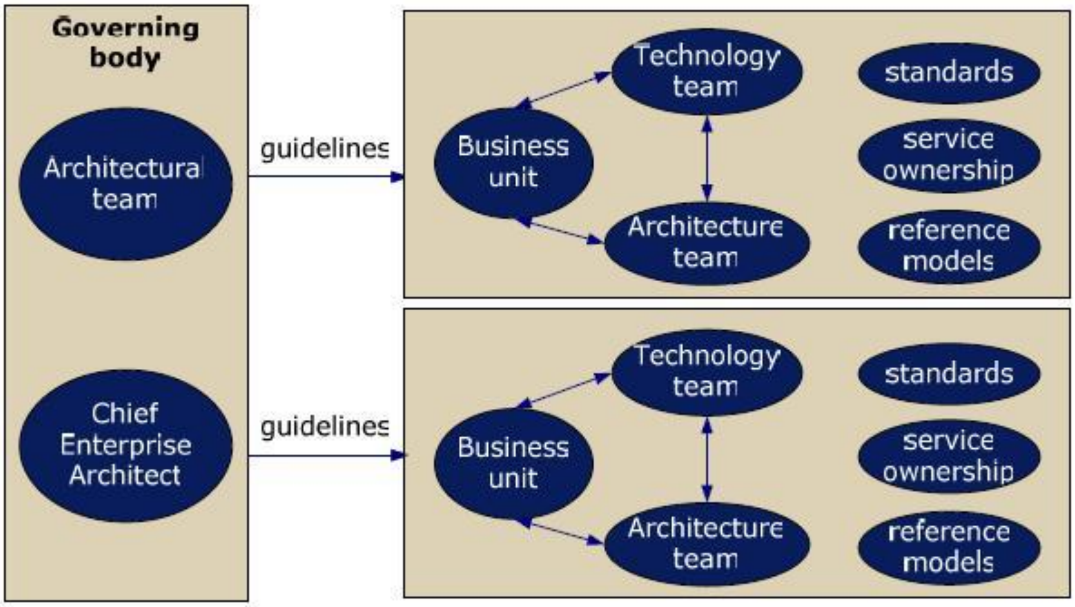


Figure 27 Distributed Governance model for SOA

Appendix E: Role in cloud computing

(CA_Technology, 2011; Eucalyptus, 2011; Schepers, 2007)

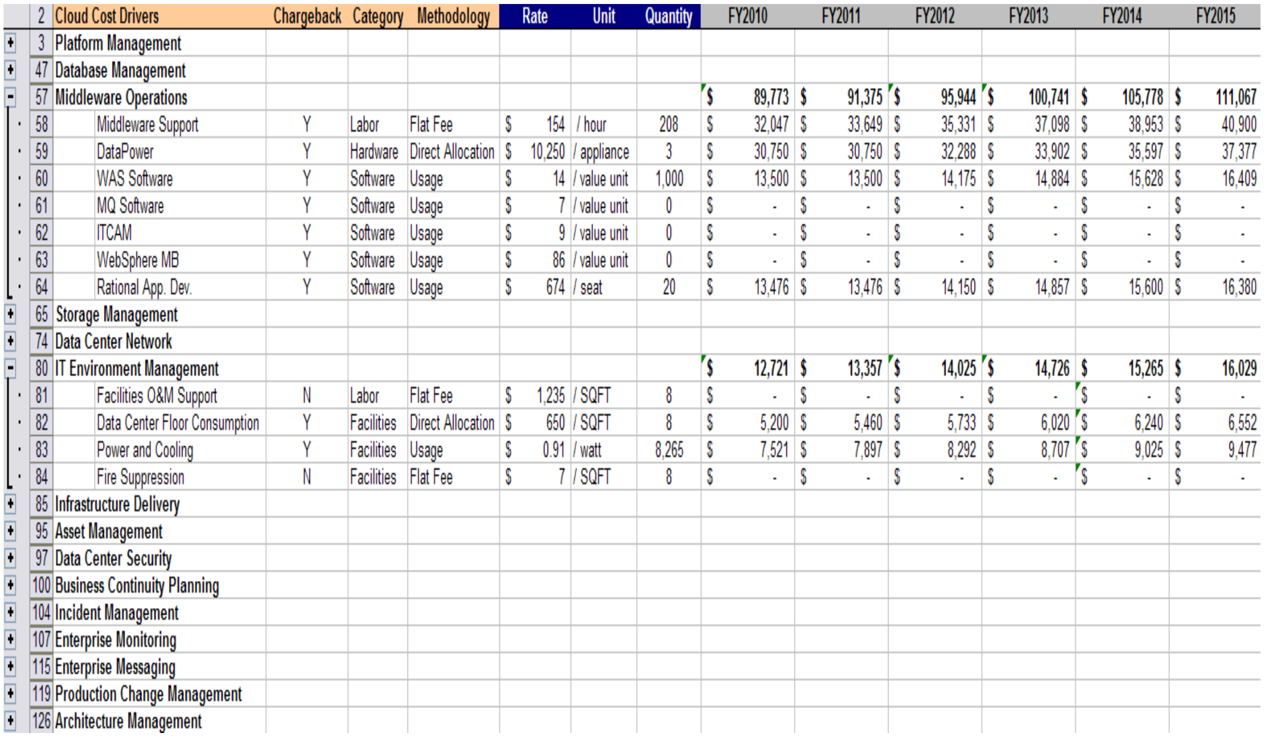
Role	Description
System Administrator (*)	Be responsible for planning , implementation and maintenance of server/hosts along with services hosted on those servers
Computer Operator(*)	Be responsible for day-to-day maintenance activities
Network Administrator (*)	Skills of network administrator are prone to be specific to the network fabric so as to ensure communication between resources and users. Individual network administrator can specialize in authentification, intrusion detection performance, network based services (e.g. file server), drivers on desktop computers.
Storage Administrator(*)	Be responsible for the design, implementation and maintenance of the storage infrastructure with an organization. Based upon the organizations choice of storage (DAS, NAS, SAN, etc), their skill sets tend to be specialized.
Data Base Administrator(*)	Be responsible for the design, implementation, and maintenance of a database
Code Developer	A Code Developer (not to be confused with a 'cloud developer') may be either a Cloud User (when they want to fully control the environment they want to use) or the End User (when they use instances created for them by the Cloud Application Architect).
Cloud Architect	The Cloud Architect will determine when and how a private cloud meets the policies and needs of an organization's strategic goals. The Cloud Architect is also responsible for designing the private cloud, understanding and evaluating the technologies and vendors needed to deploy the private cloud.
Cloud Administrator	A Cloud Administrator is responsible for the implementation, monitoring and maintenance of the cloud within the organization. Typically this role also involves the implementation of service level agreements (SLA) for

	permissions, access, quotas, etc. as required by an organization and policies. The Cloud Administrator works directly with System, Network and Cloud Storage Administrators. Besides, all the services will be categorized and maintain within one registry and cloud service manager will be responsible for the service maintenance.
Cloud Service Manager	The Cloud Service Manager designs the policies, rules and pricing model (SLA) for every cloud resource available within the organization. The SLA will need to stay consistent with the organization's policies, rules and priorities, thus the Cloud Service Manager works with the manager to receive directions and with the Cloud Administrator to implement the SLAs.
Cloud Data Architect	The cloud offers many different types of storage with possibly different SLAs associated with each of them. The Cloud Data Architect makes sure that an application in the cloud is using these different storage types appropriately, and that the application is taking full advantage of the properties of each type of cloud storage.
Cloud Storage Administrator	The Cloud Storage Administrator writes SLAs for the various groups and users (maps space, bandwidth, and reliability of the various cloud storage to the various groups/users), to ensure SLAs stay in compliance with current policies and that SLAs are met and respected. The Cloud Storage Administrator works directly with the Storage, Network and Cloud Administrators.
Cloud Application Architect	The Cloud Application Architect is responsible for adapting, porting or deploying an application to a target cloud. They work closely with end users to ensure that an application’s performance, reliability and security are all maintained throughout the lifecycle of the application. The architect's skills draw from both system administration experience (to tune the underlying OS and to act as System Administrator on instances) and from domain specific expertise (to tune the application and understand end user needs). Typically there is one architect per application domain who works closely

	with the Cloud Data Architect and the Cloud Administrators.
Cloud User	A Cloud User has access to compute resources (pre-packaged images, instances, volumes, buckets etc.) within a cloud, and is generally granted System Administrator privileges to the instances they start. Cloud Users may work with a Cloud Architect to tune specific applications, but often use the images provide to them independently.
Cloud Developer	Cloud Developers develop for the cloud infrastructure itself. This can be a developer working on a client tool or a system component. Typically Cloud Developer's work independently, though they may interact with the Cloud Administrator during debugging sessions.
Cloud Security Manager/Engineer	Be responsible for the generic security design, implementation, and evaluation of CSP's security platform, monitoring and maintenance of cloud security. This role can be overlapped with data, storage and application architects. Or an individual role can be set up for better coordination among those roles when necessary.
Business Analyst (*)	Be responsible for translating the business requirements into service definition. For example, estimate the capacity of business and cooperate with cloud architect and cloud administrator.

(Note: the roles with an asterisk are the old roles)

Appendix F: Cost Estimation Example



2	Cloud Cost Drivers	Chargeback	Category	Methodology	Rate	Unit	Quantity	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
3	Platform Management												
47	Database Management												
57	**Middleware Operations**							**$ 89,773**	**$ 91,375**	**$ 95,944**	**$ 100,741**	**$ 105,778**	**$ 111,067**
58	Middleware Support	Y	Labor	Flat Fee	$ 154	/ hour	208	$ 32,047	$ 33,649	$ 35,331	$ 37,098	$ 38,953	$ 40,900
59	DataPower	Y	Hardware	Direct Allocation	$ 10,250	/ appliance	3	$ 30,750	$ 30,750	$ 32,288	$ 33,902	$ 35,597	$ 37,377
60	WAS Software	Y	Software	Usage	$ 14	/ value unit	1,000	$ 13,500	$ 13,500	$ 14,175	$ 14,884	$ 15,628	$ 16,409
61	MQ Software	Y	Software	Usage	$ 7	/ value unit	0	$ -	$ -	$ -	$ -	$ -	$ -
62	ITCAM	Y	Software	Usage	$ 9	/ value unit	0	$ -	$ -	$ -	$ -	$ -	$ -
63	WebSphere MB	Y	Software	Usage	$ 86	/ value unit	0	$ -	$ -	$ -	$ -	$ -	$ -
64	Rational App. Dev.	Y	Software	Usage	$ 674	/ seat	20	$ 13,476	$ 13,476	$ 14,150	$ 14,857	$ 15,600	$ 16,380
65	Storage Management												
74	Data Center Network												
80	**IT Environment Management**							**$ 12,721**	**$ 13,357**	**$ 14,025**	**$ 14,726**	**$ 15,265**	**$ 16,029**
81	Facilities O&M Support	N	Labor	Flat Fee	$ 1,235	/ SQFT	8	$ -	$ -	$ -	$ -	$ -	$ -
82	Data Center Floor Consumption	Y	Facilities	Direct Allocation	$ 650	/ SQFT	8	$ 5,200	$ 5,460	$ 5,733	$ 6,020	$ 6,240	$ 6,552
83	Power and Cooling	Y	Facilities	Usage	$ 0.91	/ watt	8,265	$ 7,521	$ 7,897	$ 8,292	$ 8,707	$ 9,025	$ 9,477
84	Fire Suppression	N	Facilities	Flat Fee	$ 7	/ SQFT	8	$ -	$ -	$ -	$ -	$ -	$ -
85	Infrastructure Delivery												
95	Asset Management												
97	Data Center Security												
100	Business Continuity Planning												
104	Incident Management												
107	Enterprise Monitoring												
115	Enterprise Messaging												
119	Production Change Management												
126	Architecture Management												

Appendix G: Relationship of processes and types of cloud

	Public Cloud	**Private Cloud**
	12. Create configuration and change process: CMDB records the information as the endpoint for the service. Change process has to consider the change initiated by the providers. 20. Evaluate services: terminate contracts or take actions to get compensation from CSPs A. Manage suppliers and unify process control: eliminate redundant suppliers and unify internal and external control mechanisms B. Create service support models: both CSPs and the consumer organizations should agree with the models and activities. D. Create exit plans: mainly for public cloud services.	12. Create configuration and change processes: CMDB records the information regarding the providers as well as infrastructure elements. 15. /16. Define policy enforcement points and policy enforcement: benefit from existing SOA PEPs 20. Evaluate services: determine to use cloud-based and non-cloud based services. A. Manage suppliers and unify process control: unify internal services or components. B. Create service support models: supporting activities are only from the organizations. D. Create exit plans: mainly for public cloud services.
SaaS	12. Create configuration and change processes: CMDB should record the information to initiate the apps. 15. /16. Define policy enforcement point and policy enforcement: offer no chance for SOA PEP C. Delegate incident management: CSPs should be responsible for detecting all the incidents regarding the applications or service, including the incidents related to the underlying infrastructure.	
PaaS	12. Create configuration and change processes: CMDB records the information pertaining to the hosted apps besides the ownership information. 15. /16. Define policy enforcement point and policy enforcement: depend on cloud platform capability	

	offered by public CSPs. C. Delegate incident management: CSPs should be responsible for the incidents related to operation systems and infrastructure.	
IaaS	12. Create configuration and change processes: CMDB stores the information regarding virtualized system and upstream CIs. 15. Define policy enforcement point: own the most freedom for virtual PEP deployment; CSPs shift the boundary of control to an abstracted hypervisor, enabling virtual PEP deployment for consumer organizations. C. Delegate incident management: CSPs should be responsible for the incident regarding the infrastructure.	
Common processes	1.Define strategic cloud computing goals 2. Create high-level adoption approaches 3. Involving stakeholders 4. Determine service model and delivery model 5. Create service domains 6. Assign responsible teams 7. Establish centre of excellent 8.Ensure organizational role competency 9. Create funding model10. Define criteria for the services	11. Creating testing and validation processes 13. Manage lifecycle of services 14. Create policy processes 17. Create policy report: when policy is enforced by CSP, it is requested CSP to provide such capability to create report and consumer can access , even customized the report 18. Create SLAs 19. Monitoring compliance

Appendix H: Interview Questions

What type of cloud is using in your company? Is it private or public cloud? Is it IaaS, PaaS or SaaS?

What governance mechanism are you using in your organization now or planning to implement in your organization in the future?

Strategic plan/ business case

- Why do you introduce cloud computing?
- Who will involve in the project?
- How can you identify cloud services and determine sourcing?

Organizational Alignment

- What do you think will be changed in organizational structure when introducing cloud?
- Is there a separate organizational unit/team for cloud adoption and propagation?
- Is there any adjustment on the roles to cater for cloud computing in your organization?
- How can you allocate cloud cost within your organization?
- Is there a payment system for cloud service?
- How will cloud influence change management?

Lifecycle Management

- Is there a service catalogue implemented within organization?
- Have you implemented SOA architecture in your organization?
- Is there a registry for SOA? Can you reuse the registry for cloud computing service?
- If not, what new functions does it require for cloud computing service?
- How has testing changed to suit for Cloud Computing service?
- Do you think incident management, configuration management and service desk is important for cloud?

Policy Management

- Are there any criteria to select your cloud suppliers? (for public cloud)
- Are there rules when designing cloud services or creating service using cloud platform?
- Is there any tool to support policies? If so, what function does it perform?

Service Level Management

- Does your organization use service contract or service level agreement for cloud services?
- How is the performance and quality of cloud computing services monitored?
- Do you have any tool to monitoring usage from either public cloud or private cloud?
- How can you evaluate cloud services/instances?

Other questions:

- What do you think about outsourcing cloud governance services?
- What is the most important lesson that you have been learnt? (optional)

Appendix I: Interview Details

a) Printing company

Background

Due to the confidentiality issue, we are not allowed to mention the name of company in our research. This company is one of bigger players in the printing industry in the world. It has well matured IT supporting department for its business. Because IT department cannot provide enough capability to lines of business, some business managers choose to use public SaaS applications. Cloud is loosely used by the company now but it is not approved by top-management for company-wise adoption. This interview is conducted with one of the IT architect from the company and he is the cloud computing promoter within the company. Now he is responsible for a pilot project in order to evaluate the usage of cloud computing for the company in the future.

Strategic plan/business case

The company does not have a generic strategic plan to move their applications to cloud because of the unclear security issues in cloud. The need for cloud services originates from some specific business departments. IT department plays the role to support them. There is no communication between IT and business debarments when a cloud service has been selected and subscribed. The interviewee thinks that integration of different cloud services from various vendors will probably become an issue again as more and more cloud services are adopted in the companies without explicit standards or principles as guidelines to choose cloud services. Implementation of cloud takes slowly in the company. For example, cloud services adoption starts from a pilot project and a thorough business case analysis.

Organizational alignment

There are no specific units to propagate cloud computing within the organization. Existing departments share an implicit definition on cloud[12] in the organization. Problems will rise when more and more cloud services are adopted within the organization and it will lead to confusion on what cloud is. It is believed that the greatest impact on current roles in IT department is that most of IT engineers will be laid off since most of maintenance jobs will be outsourced to CSPs. Contract management will become important and the person who is in charge of contract negotiation or signing contract should have

[12] In author's opinion, the cloud definition they share refers to SaaS.

knowledge on laws and regulations. Cost allocation and charge back will be shared by the entire organization, which keeps the same as original charge back strategy within the organization.

Lifecycle management

Configuration management will not be changed. Incident management will be delegated to cloud services providers. The organization will rely on CSP's portal to inform CSP about the incidents or internal service desks to contact CSPs. The main focus for testing SaaS services is about integration capability with on-premises services. Change service keeps the same as the original change process within the organization; change will initiate from business department and IT department control over subscription of the services. There is no consideration on the change that is initiated by CSP. Communication channel is based on the channel provided by CSP, normally portal or CSP's corresponding email.

Policy Management

There is no clear need for policy management in the initial cloud implementation stage. The main reason lies in the reluctant of top-management support on cloud computing. And there is no data classification process in the companies currently, meaning that there is a need to create relevant policies to improve this process in the future.

SLA management

The organization highly relies on the contract to guarantee the service level from public CSPs. Actually most of the services are based on standardized contract provided by CSPs. Consumer organizations or units should evaluate the SLAs carefully before they go for cloud. The organization is not considering implementing SLA monitoring systems in the organization at the moment.

b) Centre4Cloud

Background

Centre4Cloud is a Dutch knowledge centre focusing on developing knowledge regarding cloud computing. It is cofound by Part Twente, University of Twente and Caase.com. It holds meetings and conferences to gather cloud service providers as well as cloud service clients to talk about their concerns, striving for educating them on the emergent topics and themes regarding cloud. The interviewee is the director of Centre4Cloud. He has some insightful views on what cloud governance is and has already discussed with some cloud client organizations. The discussion topic with him covers both public and private cloud services, ranging from IaaS to SaaS. According to his opinion, private cloud will not change current IT governance within organizations dramatically. However, public cloud will blur the boundary of responsibility between cloud consumers and providers and it is critical to formalize them into the contract.

Strategic plan

Generally when organizations start a new investment, they will follow traditional investment methodology to create a business case to investigate the cost and benefit. For some bigger companies, how to define a good strategic plan is still challenging. Most of organizations will consider public cloud first because it is more adaptive to the dynamic changes from business. Business managers do not have to wait for a long implementation period from IT department. Some private and hybrid solutions can be considered later to keep up with the public solutions. The decision to subscribe to the public cloud services are mainly made by the business managers with their own budgets.

Organizational Alignment

In most of organizations, there is no cooperation between Lines of business and IT department when it comes to the decisions on the cloud services. Normally, business departments bypass IT department, use their own budgets and subscribe to the services according to their business needs. Ownership of applications or services will be back to business again. Gradually, IT will lose control over the whole IT services within the organization(s). It is predicted by some people that integration will become a problem again because there is a lack of guidelines from IT department for subscribing the services. According to the expert, integration among various public cloud solutions (i.e. IaaS, PaaS, and SaaS) won't be a problem because most of cloud providers try to offer their solution towards an open cloud environment so as to enlarge their businesses. The problem will be left to how to integrate the cloud services with the on-premise ones. For private cloud, ownership of the services will still belong to IT department.

Currently most of CIOs have started to work on the principles used to guide their business departments for cloud service subscription and implementation. Role of IT department will shift to supplier managements and translation of business needs into IT requirements. IT department should be in charge of overseeing the total subscriptions to the services in order to ensure the total cost of ownership. Consumer organizations should take the responsibility to unsubscribe the redundant services in time because suppliers will be not going to inform them about the unused subscriptions.

For public services, CSPs should offer the billing detail to their consumers. For consumer organizations, they have to take care of the charge back billings within the organizations regardless of the type of services.

Lifecycle Management

There is no need for consumer organizations to manage incidents because they can do nothing if the infrastructure is not under the control of the organizations. Meanwhile it is believed that suppliers will exert their best effort to control and manage incidents and they have more knowledge regarding the topic. What consumer organizations should do is to report to suppliers about the incidents and establish a service desk to communicate with their suppliers.

Lower level of configuration will be delegated to their suppliers and consumer organizations should keep a higher level of configuration management within their organizations. For SaaS, consumer organizations should keep track on entries of the services and their relationship with other services for the configuration management. For PaaS, consumer organizations should keep track of the information for service configuration while the information for the underlying platform should be left to their suppliers. For IaaS, consumer organizations should keep track of the information used for virtual machine configuration and the downstream service configuration running on top of the virtual machines.

Lifecycle management will need a service catalogue to support it. Whether the service catalogue can be synchronized with the service catalogues from their suppliers depend on the APIs from their suppliers.

Policy Management

Whether the policies defined by consumer organizations can be enforced depends on the capability their suppliers' offers. The expert believes that policy management will be more related to the SaaS services and it is important when multiple SaaS services are composited for one process. If consumer organizations do not have the right to enforce their policy, they should delegate the corresponding responsibility to their suppliers through the contracts. Consumer organizations should provide the evidence to their suppliers that there are breaches into their services.

Service Level Management

Consumer organizations should not totally rely on the monitoring reports from their suppliers. They can monitor compliancy of SLA through their own monitoring systems or ask a third party to audit their suppliers. Nevertheless, implementing SLA system on-premise requires upfront investment, resulting in decreasing the flexibility to move out of the cloud. The expert explains that it is not necessary to invest SLA monitoring system at the very beginning unless consumer organizations have strong feeling that their suppliers have played with them.

Consumer organizations should rely on their suppliers to ensure the compliancy requirements the laws and the business regulations through contracts. They can even delegate the business continuity plan to their suppliers. However, this choice will probably be too dangerous to lead to the vendor lock in.

c) Shell

Background

Shell is a global group of energy and petrochemical companies with around 93,000 employees in more than 90 countries and territories(Shell, 2011). The interviewee is the project manager and contractor who is responsible for implementing risk and compliance in Shell. In addition, he used to be participated in several SaaS projects and had experience on the IaaS. The interview topic will focus on SaaS[13]. SaaS application management will mainly involve Business representatives from Line of Business (LoB) and Business Application Management (BAM) Department in Shell.

Strategic plan

Shell has a comprehensive lifecycle methodology for SaaS governance. It starts from business strategy on whether or not to implement SaaS. Strategic decision making will be made by LoB and BAM together. As Shell purchases the standardized SaaS solutions for their business, it declines to have everything well defined before signs the contract with their suppliers. In such a way Shell can prevent from huge extra cost for changing the functional requirement afterwards. Shell specifies a set of criteria to determine which supplier it should go for.

Organizational alignment

According to the expert, the organizational roles will not change dramatically when the organization start their SaaS solutions. In fact, Shell benefits from their extensive experience on the sourcing projects in such a cloud paradigm. The only predictable change is that the role of service manager will become more and more important due to the intensive collaboration with suppliers. Budget is still owned by the IT department but it is required them to report to the business departments about the expenses and

[13] The definition of SaaS by Shell is the same as the definition we used in our paper. Single-tenant service is normally considered by Shell for specific security requirement.

cost regarding the SaaS services. Payment to the services depends on the number of users for the services.

Lifecycle management

There is no centralized authorization or access system for all the services in Shell and it is estimated to be difficult to implement such a centralized authorization system for various services. Currently an authorization menu is created within the organization for tackling the authorization issues. Meanwhile a support model is created by Shell to clarify the supporting responsibility between LoB, BAM and suppliers. This support model should be agreed with suppliers first. According to the expert, most of supporting jobs will be delegated to the suppliers, particularly for standardized SaaS solutions. For instance, it is expected that suppliers will take care of incident management and low level configuration management. When some incidents have been detected by the suppliers, they should report to the delivery manager in Shell. High level configuration management regarding the services and service instances is still kept tracked by Shell, in which portfolio tool will be used to record the basic information for configuring the services. The information will include ownership of the applications, suppliers of the applications as well as the decision maker of the applications. Configuration management is organized as a standardized process for BAM in Shell.

The most challenge part is about change management because the SaaS solutions are standardized and it is not easy for consumers to change the functional requirement. SaaS suppliers usually provide a community for all their consumers to request for a change. Therefore change management will not only depend on the suppliers[14], but also the consumers who are using the same service. Even though consumer organizations can choose the single tenant model of SaaS solutions, the functional change will still cause a lot of money. In order to deal with periodical business/legal change requirements in the industry, a change package can be considered when consumer organizations negotiate the contract with the suppliers.

Testing for the SaaS service focuses on customer requirements, following a standardized testing framework in Shell.

Policy management

[14] Change management mainly refers to functional change and laws compliancy change.

Policies regarding business and data are defined in high level management. Data classification is well defined. Shell shares the policies in the share point to create the awareness among different stakeholders on the policies. In addition, a policy template is used for negotiating the policies among different stakeholders. Shell relies on the contract to ensure the compliancy of the services from their suppliers. Operational policy compliancy monitoring is not clear.

Service level management

Shell defines a set of criteria to select the service providers. In addition, Shell relies on a set of Key Performance Indicators to ensure the value of the services. For internal service, it tries to define Key Performance Indicators (KPI) as extensive as possible. For external services, only the important KPIs will be used in order to control the cost, because Shell have to pay for the APIs offered by the suppliers to oversee the items within the KPIs. When the SLA cannot be met, Shell will follow the service credit model to request for compensation. When negotiating the contract with the suppliers, Shell usually will specify the right to audit the suppliers. It will hire third parties such as KPMG, PWC or Deloitte to perform the audit.

If Shell found out that the suppliers have serious problems, it will terminate the contract. In such a case, internal business continuity plan should be placed to ensure the business won't be affected because of the termination.

Conclusion

Finally, we show our model to the expert and he suggests that the proposed model should specify further to the specific type of service (e.g. SaaS, PaaS, or IaaS). It would be better to associate roles with those processes to make the framework more applicable. He thinks that policy management should be in located on top of all the processes.

d) Mendix

Background

Mendix is a software provider which delivers an agile platform service(Mendix, 2011). The Toolkits and components provided by Mendix are hosted in cloud. Users of Mendix platform can create their own services on top of Mendix and host them in cloud. Application maintenance will be taken care of by Mendix. From this perspective, Mendix is PaaS providers which adopt IaaS services. The interviewee is one of the founders of Mendix. He has rich experience on their PaaS clients and understood that what is important for PaaS and SaaS clients. In addition, as the user of IaaS services, he comprehends the essence on how to control over IaaS services in order to ensure the sustainability of their own business. The topic will mainly cover IaaS service governance and PaaS service governance. Some SaaS services will be included during the interview.

Strategic Plan

The main reason for consumers to choose PaaS solution is to reduce maintenance responsibilities so that they can concentrate on the core business. In addition, PaaS solution enables them to implement their solutions within a limited time frame. Normally consumer organizations will start a prototype within their organizations and adopt an incremental approach for cloud solutions.

Organizational Alignment

The adoption of cloud computing will reduce the responsibilities from IT department. The responsibility for IT will shift to check SLAs and make plans to get out of cloud without affecting the business. In a tactical level, IT department is likely to pay attention to the security issues. Mendix pays their IaaS suppliers in terms of the usage and it charges back from their clients on the basis of the software licenses model, in which the cost is set up based on the number of concurrent users. According to the interviewee, the final cost will be allocated to business units within the consumer organizations.

Lifecycle Management

For Mendix, supporting flexible lifecycle management is one of the advantages of the PaaS and SaaS solutions from Mendix. Instead of requesting through a common community from the providers, Users of Mendix can rely on the lifecycle portal to change the functions of their services easily. At the same time, it is critical for the consumer organizations to specify relevant owners and activities to complete the whole change process. For example, they can define who can make the decision for a change, how to collect feedback and how to prioritize the decision and so on. Authorization management will be related to the whole lifecycle, such as authorization on requirement gathering, functional design and application itself. When the cloud services are designed to support a whole process and multiple suppliers are used, consumer organizations should manage the dependency of the services as well.

The ITIL framework will not change from the perspective of clients and it can still be used to standardize the processes. For instance, there is always configuration management in the consumer organizations but the management will be considered at higher level. For SaaS and PaaS users, incident management can be delegated to their cloud providers. Nevertheless, consumer organizations should get involved to provide some contextual information so that the providers can deal with incidents correctly. Consumer organizations should check and audit the incident reports sent by their providers to prevent from loss. There is no need to have a thick governance body for incident management.

For Mendix, PaaS solution is their core business and its own platform service provision highly relies on the IaaS suppliers. Therefore the expert believes that business continuity plan plays an important role to ensure sustainability of the business. The control mechanism Mendix has adopted is to use multiple suppliers and create their own data centers to prevent from single point of failure.

Testing on cloud applications or service should concentrate on performance testing. Security testing is important. Nevertheless, it is believed that conducting security testing from consumer organizations is nearly impossible since security testing on cloud should go through the whole layers(i.e. from SaaS to IaaS).

Policy management

Policy management seems more related to SaaS layer rather than PaaS or IaaS layer. SaaS end user organizations should implement a policy manager to integrate with the SaaS services from partner providers. Policy management is important for big organization. However, it is very rare to see organizations implement policy management in practice. In generally, policy management is enforced in process level and conducted manually. Centralized policy management is quite difficult and complex. Most of the policy management is kept at higher level.

SLA Management

To its client, Mendix relies on a comprehensive contract to clarify the responsibilities Mendix should take and the responsibilities its IaaS suppliers should take. Mendix allows their clients to choose the IaaS providers they preferred and it will provide some advices to help the clients for the final decision. Clients can receive the reports on the services through the dashboard or the service desks set by Mendix.

To the IaaS suppliers, Mendix follows the standardized contract provided by the IaaS suppliers. Nevertheless, it established a set of control mechanisms within the organizations to monitor the suppliers. SLA and cost are the main monitoring items. According to the expert, monitoring the virtualized servers from the IaaS suppliers is the same as monitoring traditional servers. Even though the IaaS suppliers offer a portal to check their monitoring results, Mendix prefers to implement the SLA monitoring on its own. By establishing its own monitoring mechanism, Mendix can take the actions more quickly when problems have been detected. Outsourcing SLA is not a choice for controlling over IaaS providers because Mendix has to implement another control mechanism over the control parties, leading to a more complex governance situation.

Conclusion

Finally, we show our model to the expert. He suggests that a maturity model should be added into the model so that it can be applied to different organizations. In his opinion, the strategic plan and organizational alignment sections should be incrementally adjusted to align with the proposition of cloud. It seems to be too immature to implement a comprehensive governance structure within organizations at the moment. Most of the organizations just start to implement a pilot to test the value of cloud. Flexible service lifecycle management is thought to be important because it fits the agility proposition of cloud. Consumer organizations should establish processes to support the management. Meanwhile, suppliers should also offer the technological capability to support it. Policy management is more important for SaaS rather than PaaS or IaaS.

e) Novay

Novay is a Telematics Institution and it works with multiple industrial partners and universities to deliver innovative ICT services(Novay, 2011). The interviewee is one of the managers who used to participate in several cloud projects before.

Novay started to work with cloud 2 years ago. Currently they are developing an Open Health Service and host them in an external cloud. This service used to be hosted on top of Amazon Cloud Servers[15]; however, Novay decided to move back the service to a Dutch Datacenter because of the compliancy requirements from the Dutch Law. Governance mechanisms are relatively simple within the organization at the moment.

[15] The main cloud service they use is IaaS services and PaaS

Cost is the main driver for Novay to consider cloud. There is no systematic high level adoption approach. Currently there is only a small group of people assisting cloud implementation. Contractual agreement is the main mechanism Novay uses to control their suppliers and ensure the quality of the service. SLA and ownership of data are the main concerns for Novay.

Novay has followed the traditional testing approach for cloud services, in which integration and security testing are the main concerns. Change management mainly relies on the frequent collaboration with their customers and suppliers. If there are major changes from their suppliers, Novay will be notified beforehand so that it can perform some critical impact analysis. In the case that the suppliers' services failed or the SLA cannot be met, Novay has nothing to do with the situation. Nevertheless, Navy will make use of the service credits from their suppliers to compensate for the lost.

There is no specific policy management processes within Novay since most of the policies rely on the requirements from their customers. Novay follows the requirements from their clients to design routing message with other cloud service components carefully.

As stated before, contract and SLA are the main control mechanisms. However, instead of implementing their own SLA monitoring tools, Novay simply rely on the information provided by the cloud suppliers.

f) Eurocloud

Background

Eurocloud is a business network striving for promoting SaaS and Cloud Computing in European Countries(Eurocloud, 2011). The interviewee is the vice chairman Eurocloud Netherland, General Director of Eurocloud Europe, European SaaS & Cloud Computing Community. He used to be the CIO at Kwik Fit in the Netherlands. Currently he runs his own consulting company and offers solutions on the topics around organizational structure issues, business transformation and process design. Currently the interviewee has a strong focus on the necessary changes in business model for cloud computing. The interview topic focuses on the SaaS cloud computing services.

Strategic Plan

Change of the business model is the core value proposition from cloud computing. It is also the core driver that consumer organizations consider adopting cloud computing. The key to ensure the value of cloud computing adding into the business is to make sure that total cost of ownership (TCO) should be put into place before introducing the cloud. In such a way, ROI can be calculated. Nevertheless, most of organizations have not owned a method to examine their TCO against the value of cloud computing[16] at the moment.

Organizational Alignment

Comparing with traditional on-site services, cloud computing enables business to look for the services they need on-line instead of requesting IT department to supply the services. The problem is that IT still holds the responsibility to support services. If they don't know what type of services the business departments will subscribe, it is hard for them to handle data portability, interoperability and data privacy control. In the interviewee's opinion, IT department should not be handing technical issue anymore. The main responsibility of IT department should shift to contract management. In addition, IT should define policies or guideline for business departments. For example, IT should define how to handle data, what type of cloud services they can subscribe. This requires IT personnel to understand their own business rules, their providers' business rules and laws. Main roles for cloud services within consumer organizations will include contract manager, information manager and change manager.

Within the organization(s), business departments hold the budget and they own the services. Business department will specify the policies in relation to the privacy requirements and business regulations. By following the guidelines defined by IT department, business department can decide what programs/infrastructure they will need. Contract manager should consult with business managers, define detailed SLAs and make sure where the data is resided and compliancy of the policies. Contract manager will get the invoice and charge back to business departments.

Lifecycle Management

Incident management and configuration management should be delegated service providers. It is believed that service desk will become more and more important in the era of cloud. Change management will be still part of the responsibility for consumer organizations. Change managers should cooperate with contract manager to ensure the value of changing some of the cloud computing services. They should make sure appropriate education on related employees. Conversion of the services should not influence the business. As for incident management and configuration management from ITIL, they should be delegated to service providers. When the incidents have escalated to a problem and service

[16] One out of 80 organizations attending IDC seminar on cloud governance in Amsterdam 2011 admits that they have TCO in their organization.

providers need to change their service to cope with the problem, the providers should notify the contractor from consumer organizations to prepare for the change.

Policy Management

In organizational alignment section, policy management involves two streams. One is that business department should define policies regarding the data privacy. The other is that IT should define policies to guide the business departments to subscribe to the cloud services.

SLA Management

The Safe Harbor Policy from US and Digital Agenda from Europe are the two main policies on the data privacy. Contract managers can specify in the contract that supplier should comply with those two policies when they negotiate with their suppliers.

In the case that services from suppliers fail, consumer organizations should have a business continuity plan in place to avoid business loss. Traditionally, consumer organizations can replicate the data and services on-site to prevent from the single point of failure. Nevertheless, this solution will lead to reducing the TCO from cloud and diminishing the value from cloud. Another option is that consumer organizations can delegate the business continuity plan to suppliers through the contract.

Consumer organizations cannot simply rely on the information provided by their suppliers, they should put some monitoring control mechanisms to make sure the compliancy. For example hire a third party organization to audit their suppliers. Some third party groups have already had a comprehensive auditing capability on the cloud SaaS service providers, including KPMG and EuroCloud.

g) Logica

Introduction on Logica has been done at the beginning of the thesis. The main cloud service used by Logica is Microsoft Azure, a cloud Platform-as-a-Service. The interviewee is the software architect who is responsible for contacting with Azure datacenter in Logica. The interview topic will be around platform as a service.

For PaaS cloud service, consumer organizations will be mainly the software developing companies and/or IT department. The reason why Logica considers the Azure public cloud solution is to reduce cost and deployment time. According to the expert, it is more flexible to change services because developers can scale the applications easily to suit for the business requirements from their clients.

Most of roles in developing team will not change. But the organization should educate the developers to be aware of the cost and security. There is one coordinator who is responsible for cloud activities within Logica. The job performed by the coordinator is to facilitate communication among different departments and improve knowledge sharing within the organization. Logica pays Microsoft Azure service based on monthly subscription fee and they charge back their customers through monthly fixed cost. Even though cloud promotes pay-by-usage business model, most of customers prefer fixed cost payment on the services. How Logica can benefit from the new business model from cloud is still under investigation.

Testing is almost the same as traditional web-based service testing in cloud. Security testing plays an important role on cloud services. Configuration management on the application level is the same while hardware configuration is more flexible in cloud. Change management is realized through the administration portal from Azure. Incident management depends on Azure and service desks from Logica has connected to the service desks from Azure and helped to solve the problems or questions from the end user of the services.

Logica has created a comprehensive SLA or contract with their customers; SLA monitoring is implemented to ensure the SLAs can be met. Since the services are running on top of the infrastructure services from Microsoft Azure, when the SLAs have been monitored, the service level from the Azure has been included as well. Logica have arranged an exit plan through making a copy of data on-premise. In the case that service is not available from Microsoft, applications can be moved back to on-premise infrastructure and it won’t take a lot of time to make the service executable again.

	Strategic Plan	**Organizational Alignment**	**Service Lifecycle Management**	**Policy Management**	**SLA management**
Printing company	Top management is reluctant to use cloud. Cloud service is subscribed by LoB individually. No guideline or standard for cloud service subscription.	No governance team or knowledge centre for cloud. Most of software engineers will be laid off due to the adoption of cloud. Contract management will be important. Cost allocation will be shared by LoBs.	Testing focuses on integration test with on-premise services. Configuration management will only change the entry of service. Incident management will mostly rely on suppliers through their portal. Internal support desk will assist communication with suppliers.	No specific policy management. No data classification process and be expected to improve in the future.	Contract management will have to get involved with a lot of law issues. No plan to implement SLA monitoring mechanisms themselves.
Centre4Cloud	Business case is still considered when it comes to cloud investment. Be adaptive to business and short delivery time are the main reasons to choose cloud. Business manager makes decision to	Lack of cooperation between IT and LoB on decision making. Integration will not be problems due to the trend to open cloud environment. Ownership of service will be back to business units.	Incident management is not necessary while setting up service desk to communicate with suppliers will be important. Configuration management is only considered in higher level. Low level job is delegated to	Enforcing you own policies link to your service depends on suppliers. Policy management is more related to SaaS services. Normally use contract to clarify responsibilities.	It is expensive to implement own SLA monitoring than using supplier's monitoring report. Diminish the value of dynamic value of cloud. Business continuity plan should be

	cloud with their own budget.	Ownership of private cloud will not change. Roles of IT department will shift to supplier's management and business requirement translation. Charging back strategy has to be tailed again.	suppliers. Service catalogue is critical to set up to keep track on the services.		arranged by organization themselves.
Shell	No change and shell holds a comprehensive strategic plan. Business and IT department are well coordinated.	Responsibility of service manager will increase. No centre of excellent for cloud.	Authorization management is also an issue for Shell, centralized authorization is impossible. Change management is hard for standardized SaaS solution and an extra change package is considered when negotiating contract. Supplier should take care of Incident management.	Policy regarding business and data are well defined in higher level management. IT department is responsible to define policy on how to use services, which can use service. Policy enforcement are contractual bound, daily basis of policy tracking is not clear.	SLA tools are used to monitoring providers. They try to minimize the number of KPI to control over cost. Service credit model is applied to get reasonable compensation from suppliers. Hire third party to audit suppliers.

			Configuration management only takes care of ownership relationship and portfolio management. Testing focuses on customer requirement.		
Mendix	Main reasons for clients to choose their PaaS solution are to reduce maintenance burden and lead time. Incremental adoption and pilot study is adopted to enhance successful rate.	IT responsibility of clients will decrease. Main responsibility is to check SLA and design exit plan.	Change management on functional requirement should be arranged in organization. PaaS suppliers should provide a lean change capability to support it. Configuration management will be conducted in higher level. Dependency is related to architecture in general, not cloud-specific. For PaaS and SaaS users, incident management should be delegated to their	Policy management is more related to SaaS layer rather than PaaS and IaaS layer. Implement policy enforcement will be only applicable in higher level. Centralized policy management is impossible.	Mendix uses multiple IaaS suppliers and has their own datacenter to mitigate the risks using cloud. SLA monitoring tools are used by Mendix. An implicit process to compare reports from their suppliers. Outsource SLA control will make the control complicated. To their clients, a detailed layer responsibility is specified. Availability will

			suppliers. User should provide contextual info. To assist management. Testing focuses on performance. Security testing for SaaS will be impossible.		be sent to their customer through dashboard.
Novay	No specific strategic plan. Pilot study and incremental approach is adopted. Try not to use cloud component from other suppliers.	A small team is responsible for cloud maintenance and coordination.	Main criterion to choose supplier is security and compliance. Configuration management keeps the same. Change management is well organized due to high frequent communication with their suppliers and clients. Testing focuses on integration and security.	No specific policy process. Follow customer's data requirements and keep control over interaction message when external cloud component is used.	Currently there is no self-built SLA monitoring. Rely on contract and the information provided by suppliers. Plan to use the tools to monitor SLA when the business is getting bigger. No business continuity plan and rely on service credit to compensate the loss on customers.
EuroCloud	Make sure TCO is in place so as to calculate ROI of cloud computing to	IT should not handle technical issue but concentrate on contract	Incident management and configuration management should be	Business department should define policy regarding data privacies	Contract manager is responsible for negotiation and ensure that

	ensure its value	management. Business holds the budget and owns the services. Main roles for cloud computing will lie in contract manager, change manager and information manager.	delegated providers. Change management should be handled by client organization and cooperation with suppliers.	and other business rules on the services. IT department should define policies or principles on how to handle data, how to subscribe cloud services.	business policies and their data privacy requirement can be guaranteed by their suppliers. Auditing suppliers can be realized through third parties such as KPMG. Business continuity can be delegated to providers through contract.
Logica	The reason to use Azure is to reduce cost and lead time to the market.	Most of roles in developing team have not changed. Cloud coordinators are useful for knowledge sharing. Logica pays for their cloud service on subscription basis and charges their customer at fixed price.	Testing is similar to traditional web-service testing. Security testing should be paid more attention in cloud. Infrastructure change for the application will follow the process from supplier's administrative portal. Incident management should be	Policy should take care how to deal with data sensitivity within organization.	Monitor SLA with regard to the services on top of cloud platform to make sure that SLA made with customers are met. Business continuity can be guaranteed through its own data replication on-site. When supplier's service fails,

			delegated to suppliers. Service desk is getting more and more important.		moving back to on-premise infrastructure does not take a lot of time.

Table 10 Summary of Interview